

On the Optimality of Secret Key Agreement via Omniscience

Chung Chan, Manuj Mukherjee, Navin Kashyap and Qiaoqiao Zhou

Abstract—For the multiterminal secret key agreement problem under a private source model, it is known that the maximum key rate, i.e., the secrecy capacity, can be achieved through communication for omniscience, but the omniscience strategy can be strictly suboptimal in terms of minimizing the public discussion rate. While a single-letter characterization is not known for the minimum discussion rate needed for achieving the secrecy capacity, we derive single-letter lower and upper bounds that yield some simple conditions for omniscience to be discussion-rate optimal. These conditions turn out to be enough to deduce the optimality of omniscience for a large class of sources including the hypergraphical sources. Through conjectures and examples, we explore other source models to which our methods do not easily extend.

Index Terms—secret key agreement, omniscience, multivariate mutual information, Wyner common information, Gács-Körner common information.

I. INTRODUCTION

We consider the secret key agreement problem of [1], possibly with trusted and untrusted helpers, as well as silent users as in [2]. Two or more users want to agree on a secret key after observing some discrete memoryless correlated private sources that take values from finite alphabet sets. The users are allowed to discuss (possibly interactively) with other users publicly over a noiseless authenticated broadcast channel. After the discussion, each active user (who is not a helper) attempts to compute a common secret key that is asymptotically uniformly random and independent of the public discussion as well as the private sources of the untrusted helpers. The maximum achievable key rate is called the *secrecy capacity* C_S , and the minimum public discussion rate required to achieve the

capacity is called the *communication complexity* R_S . While C_S was characterized in [1], a single-letter characterization for R_S remains open, and is the main focus of this work.

For the general source model with possibly trusted helpers, it was shown in [1] that R_S can be upper bounded by the smallest rate R_{CO} of communication for omniscience (CO), the state where every active user can asymptotically recover the entire private source. More precisely, the proposed capacity-achieving scheme is through omniscience, i.e., by having users communicate in public until every user recovers the entire private source and then extract a common secret key as a function of the recovered source that is asymptotically independent of the public discussion. While this omniscience strategy was shown to be capacity-achieving, it was also pointed out in [1] to be suboptimal in the sense that strict inequality $R_S < R_{CO}$ is possible.

For the general source model with two users but no helpers, there is a multi-letter characterization of R_S in [3], and an example was also given where non-interactive discussion, i.e., the usual independent source coding scheme over a source network [4], was shown to be suboptimal. A special hypergraphical private source model [5] was also considered in [6] in the multi-user case but without helpers, and R_S was characterized when the discussion is non-asymptotic and restricted to be linear functions over a finite field. However, the expression was NP-hard to compute, and it was shown to be a loose upper bound for R_S in the asymptotic model [6].

While a single-letter characterization remains unknown even for the two-user case, simpler questions about the communication complexity may be asked. In the no-helper case, [7] considered the refined condition of *omnivocality*, which is the scenario when every user must discuss at strictly positive rate to achieve the secrecy capacity. The result was further refined by [8] to a set of vocality conditions that describes whether a particular user needs to discuss at strictly positive rate to achieve the capacity. These conditions were conjectured to be necessary and sufficient, but the conjectures turn out to be easy to resolve (see [9–11]) using

- 1) the characterization of the secrecy capacity in [2] in the no-helper case under the additional vocality constraints that a given proper subset of the users, called the *silent users*, are not allowed to discuss, and
- 2) the properties of the multivariate mutual information (MMI) [9] that was shown in [5, 12] to be equal to the secrecy capacity in the no-helper case.

In this work, we consider a different question that turns out to be easier to address than the problem of characterizing R_S :

Parts of this work were presented at the 2016 IEEE International Symposium on Information Theory (ISIT 2016), Barcelona, Spain, and at the 2016 IEEE Information Theory Workshop (ITW 2016), Cambridge, UK.

C. Chan (email: cchan@inc.cuhk.edu.hk), and Q. Zhou are with the Institute of Network Coding at the Chinese University of Hong Kong, the Shenzhen Key Laboratory of Network Coding Key Technology and Application, China, and the Shenzhen Research Institute of the Chinese University of Hong Kong. Their work was supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08), and supported partially by a grant from Shenzhen Science and Technology Innovation Committee (JSGG20160301170514984), the Chinese University of Hong Kong (Shenzhen), China. The work of C. Chan was supported in part by The Vice-Chancellor's One-off Discretionary Fund of The Chinese University of Hong Kong (Project Nos. VCF2014030 and VCF2015007), and a grant from the University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. 14200714).

N. Kashyap (nkashyap@ece.iisc.ernet.in) and M. Mukherjee (manuj@ece.iisc.ernet.in) are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012. Their work was supported in part by a Swarnajayanti Fellowship awarded to N. Kashyap by the Department of Science & Technology, Government of India.

When is omniscience optimal for achieving secrecy capacity, i.e., when is $R_S = R_{CO}$? This question was raised in [13] in the no-helper case, and a sufficient condition for the optimality of omniscience was given in the special case of the pairwise independent network (PIN) model defined in [14, 15]. The result was based on a lower bound on R_S that extended the result of [3] to the multiterminal case. The sufficient condition was later shown to be necessary in [16]. However, the result does not apply to more general source models beyond PIN, such as the hypergraphical model. Moreover, the problem formulation in [16] precludes additional randomization in the public discussion; it was conjectured (but not proved) there that randomization does not affect R_S . In this work, we overcome the above weaknesses and the following are the contributions:

- 1) Derive single-letter lower and upper bounds for a general source model possibly with helpers and silent users, and with private randomization allowed.
- 2) Obtain easily computable sufficient as well as necessary conditions for the optimality of omniscience.
- 3) Discover more scenarios beyond PIN for which R_S can be characterized by R_{CO} .
- 4) Give concrete examples where the sufficient/necessary conditions can fail to be necessary/sufficient respectively, which may inspire further improvement on the bounds.

The results in the no-helper case will be stated more meaningfully using the MMI in [9] that extends Shannon's mutual information to the multivariate case. R_S can be viewed as a measure of discord of the mutual information, and the public discussion viewed as an irreversible process of making the mutual information among the users less and less discordant until a consensus is achieved wherein the mutual information among the users is consolidated as a common secret key without further discussion.

The paper is organized as follows:

- The main ideas of the paper are motivated in Section II with some simple examples. Some background knowledge in secret key agreement is assumed.
- Section III formulates the problem by introducing 1) the secret key agreement problem with different types of users in Section III-A, and 2) the capacity-achieving omniscience strategy in Section III-B.
- For ease of understanding, the main results are introduced in two stages. The basic scenario with no helpers or silent users is first tackled in Section IV, where the fundamental proof techniques can be conveyed without much notational complexity.
- In the second stage, the proof techniques are extended to the general scenarios with helpers and silent users. We first derive single-letter upper bounds on the communication complexity in Section V, which follows directly from the achievability result of the omniscience strategy

in Section V-A or indirectly by a change of scenario in Section V-B.

- Single-letter lower bounds for the general scenario are derived in Section VI. We extend the proof techniques in an information-theoretically meaningful manner, by introducing in Section VI-A some properties of a fractional partition information measure useful for proving converse results. The general lower bound is then derived in Section VI-B using the converse proof techniques. The tightness of the bound is investigated in Section VI-C, VI-D, VI-E and VI-F, where the general lower bound is specialized and strengthened to different forms under different scenarios and for the hypergraphical source model.
- Section VII explain the challenges that remain. The current techniques was shown to be limited for a non-hypergraphical source in Section VII-A, resolving the conjecture in [17]. Potential improvements of the results are conjectured and illustrated in Section VII-B.

Proofs of the results are included in the appendices.

II. MOTIVATION

The purpose of this section is to present some simple motivating examples. It is assumed that the reader is familiar with the basic problem of multiterminal secret key agreement, as introduced in [1].

We first introduce the idea of secret key agreement informally by the following example where omniscience is strictly suboptimal $R_S < R_{CO}$.

Example 2.1 Let X_0, X_1 and J be uniformly random and independent bits. Suppose user 1 and 2 observe the private sources

$$\begin{aligned} Z_1 &:= (X_0, X_1) \quad \text{and} \\ Z_2 &:= (X_J, J) \end{aligned}$$

respectively, where X_J is equal to X_0 if $J = 0$, and equal to X_1 otherwise. A secret key agreement scheme with block length $n = 1$ is to have

$$\begin{aligned} F &:= F_2 = J \quad \text{and} \\ K &:= X_J, \end{aligned}$$

i.e., have user 2 reveal J in public so that both users can compute and use X_J as the secret key, which can be shown to be independent of F as desired. This is capacity-achieving because the secrecy capacity in the two-user case is the mutual information [1]

$$C_S = I(Z_1 \wedge Z_2) = 1$$

and so the communication complexity R_S is at most $H(J) = 1$. Note that omniscience has not been attained because $H(Z_1|Z_2) > 0$ (and so user 2 cannot recover Z_{1-J} unless user 1 also communicates). More precisely, from [1], the minimum rate of communication for omniscience is

$$R_{CO} = H(Z_1|Z_2) + H(Z_2|Z_1) = 2 > 1 \geq R_S.$$

In particular, to achieve omniscience, user 1 needs to discuss at rate at least $H(Z_1|Z_2)$ while user 2 needs to discuss at rate at least $H(Z_2|Z_1)$, hence the R_{CO} formula above. \square

R_S is difficult to compute even for the above example. Nevertheless, there is a simple condition for omniscience to be optimal in the general two-user case, which is obvious from [3, 18, 19]:

Proposition 2.1 *For the two-user case, $R_S = R_{CO}$ iff $R_{CO} = 0$, i.e., $H(Z_1|Z_2) = H(Z_2|Z_1) = 0$ where Z_i are the private source observed by user $i = 1, 2$.* \square

PROOF The “if” case is trivial and follows from the bound $R_S \leq R_{CO}$. To prove the “only if” case, note that the capacity-achieving scheme of [18, 19] has a discussion rate of $\min\{H(Z_1|Z_2), H(Z_2|Z_1)\} \in [R_S, R_{CO}]$. $R_S = R_{CO}$ implies that the minimum is $R_{CO} = H(Z_1|Z_2) + H(Z_2|Z_1)$ [1], which happens iff $H(Z_1|Z_2) = H(Z_2|Z_1) = 0$, or equivalently, $R_{CO} = 0$. \blacksquare

One of our goals is to extend the above condition to the multiterminal case to discover new scenarios where omniscience is optimal:

Example 2.2 Suppose user 3 observes the private source

$$Z_3 := Z_1 \oplus Z_2, \quad (2.2)$$

which is the XOR of two uniformly random and independent bits Z_1 and Z_2 observed by user 1 and 2 respectively. In the no-helper case, a secret key agreement scheme is to have each user $i \in \{1, 2, 3\}$ observe $n = 2$ i.i.d. samples, Z_{i1} and Z_{i2} , of its private source, and then choose

$$\begin{aligned} F &:= (F_1, F_2, F_3) = (Z_{11} \oplus Z_{12}, Z_{22}, Z_{31}) \quad \text{and} \\ K &:= Z_{11}. \end{aligned}$$

It can be shown that K is independent of (F_1, F_2, F_3) and therefore secured. User 1 can recover the key trivially, while user 2 and 3 can recover it from their observations and the public discussion by computing respectively

$$\begin{aligned} F_3 \oplus Z_{21} &= K \quad \text{and} \\ F_1 \oplus F_2 \oplus Z_{32} &= K \end{aligned}$$

by (2.2). This is capacity-achieving because the secrecy capacity is upper bounded by [1, (26)] as

$$C_S \leq \frac{1}{2} \left[\sum_{i=1}^3 H(Z_i) - H(Z_1, Z_2, Z_3) \right] = \frac{1}{2},$$

which is achieved by the current scheme. Omniscience is also attained because $H(K, F) = 4$, which is the randomness of the entire source sequence (Z_1^n, Z_2^n, Z_3^n) . Since every user can observe F and recover K , they can also recover the entire source sequence. \square

The above example belongs to a more general finite linear source model [12] instead of the PIN or hypergraphical source model considered in the existing works of [16, 20]. Our result will imply $R_S = R_{CO}$ for this example.

III. PROBLEM FORMULATION

While the no-helper case provides much intuition into the problem of communication complexity, we will consider the more general scenario with helpers and silent users, which unveils new challenges and inspires new techniques. More precisely, we will extend the secret key agreement protocol of [1] without silent users and that of [2] without helpers to study the problem of communication complexity in the general case with both helpers and silent users. It will be seen that the secret key agreement scheme via omniscience from [1] needs to be modified, in particular, to minimize the discussion of the untrusted users, and to incorporate silent users as in [2].

A. Communication Complexity

The following specifies all the user sets involved in the secret key agreement problem:

User sets

V : The ordered finite set of all users, where $|V| \geq 2$. Unless stated otherwise, we assume $V = [|V|]$ where

$$[m] := \{1, \dots, m\} \quad (3.1)$$

for any positive integer $m \geq 2$.

$A \subseteq V$: The subset of $|A| \geq 2$ users, called the active users (who want to share a common secret key among themselves). $V \setminus A$ is called the set of helpers (who help the active users share the secret key).

$D \subseteq V \setminus A$: The subset of untrusted helpers (whose observations are wiretapped). The subset $V \setminus A \setminus D$ consists of the trusted helpers.

$S \subseteq A \cup D$: The subset of silent users (who cannot speak in public). $V \setminus S$ consists of the vocal users. Without loss of generality, we assume $V \setminus S := [|V \setminus S|]$ unless stated otherwise.

The users have access to a private (discrete memoryless multiple) source denoted by the random vector

$$Z_V := (Z_i \mid i \in V) \sim P_{Z_V} \quad \text{taking values from} \quad (3.2a)$$

$$Z_V := \prod_{i \in V} Z_i, \quad (3.2b)$$

which is assumed to be finite. Note that, for notational convenience, we use capital letter in sans serif font for random variables and the same capital letter in the usual math italic font for the alphabet sets. P_{Z_V} denotes the joint distribution of Z_i 's.

The vector (A, S, D, V, Z_V) of user sets and private source is called a scenario. Given a scenario, the vocal users discuss in public until the active users can recover a secret key of their choice that is secured against a wiretapper who can listen to the public discussion and wiretap the private source of the untrusted users. The protocol can be divided into the following phases for ease of exposition:

¹For sets E, F, G , we will use the notation $E \setminus F \setminus G$ to denote the set difference $(E \setminus F) \setminus G$.

Secret key agreement protocol

Private observation: Each user $i \in V$ observes an i.i.d. sequence

$$Z_i^n := (Z_{it} \mid t \in [n]) = (Z_{i1}, \dots, Z_{in})$$

of its private source Z_i (3.2) for some block length n .

Private randomization: Each user $i \in V \setminus D \setminus S$ generates a random variable U_i independent of the private source, i.e.,

$$H(U_{V \setminus D \setminus S} \mid Z_V^n) = \sum_{i \in V \setminus D \setminus S} H(U_i). \quad (3.3)$$

(We will show in Proposition 3.1 that the silent and untrusted users need not randomize for the problem of interest.) For convenience, we let

$$\tilde{Z}_i := \begin{cases} (U_i, Z_i^n) & i \in V \setminus D \setminus S \\ Z_i^n & i \in S \cup D \quad (\text{otherwise}) \end{cases} \quad (3.4)$$

be the entire private observation of user $i \in V$.

Public discussion: Using a public authenticated noiseless channel, the vocal users broadcast some messages in a round-robin fashion interactively for a finite number of rounds. More precisely, at time $t = 1, \dots, r$ for some positive integer r , the vocal user $i \in V \setminus S$ broadcasts to everyone a function of its accumulated observations, denoted as

$$F_{it} := f_{it}(\tilde{Z}_i, \tilde{F}_{it}) \quad \text{where} \quad (3.5)$$

$$\tilde{F}_{it} := (F_{[i-1]t}, F_{V \setminus S}^{t-1}), \quad (3.6a)$$

which includes the previous messages $F_{[i-1]t} := (F_{jt} \mid j < i)$ broadcast in the same round and the messages $F_{V \setminus S}^{t-1} := (F_{V \setminus S \tau} \mid \tau < t) = (F_{i\tau} \mid i \in V \setminus S, \tau < t)$ broadcast in previous rounds. Note that, unless otherwise stated, we assumed without loss of generality that the discussion in each round is in the ascending order of $i \in V$ and that $[i-1] \subseteq V \setminus S$. We also use

$$F_i := (F_{it} \mid t \in [r]) \quad \text{and} \quad (3.6b)$$

$$F := (F_i \mid i \in V \setminus S) \quad (3.6c)$$

to denote, respectively, the vector of all messages from user $i \in V \setminus S$ and all vocal users.

Key generation: Each user $i \in A$ is required to recover a common secret key from his accumulated observations in the sense that

$$\lim_{n \rightarrow \infty} \Pr \left(\exists i \in A, K \neq \theta_i(\tilde{Z}_i, F) \right) = 0 \quad (3.7)$$

for a random variable K , called the secret key, and some function θ_i that recovers the key from the entire observation of user $i \in A$. The secret key K must also be nearly uniformly random and independent of the wiretapper's observations (F, \tilde{Z}_D) , i.e.,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \left[\log |K| - H(K \mid F, \tilde{Z}_D) \right] = 0, \quad (3.8)$$

where K denotes the finite alphabet set of possible key values.

The secrecy capacity is defined as

$$C_S := \sup \liminf_{n \rightarrow \infty} \frac{1}{n} \log |K| \quad (3.9)$$

where the supremum is taken over all key rates achievable for the given scenario (A, S, D, V, Z_V) but with any sequence (in n) of choices of other parameters respecting the constraints on private randomization (3.3), interactive public discussion (3.5) as well as recoverability (3.7) and secrecy (3.8) of the secret key. A C_S -achieving scheme corresponds to a sequence of choices with achievable key rate equal to the capacity. If the supremum in (3.9) and the constraints (3.7) and (3.8) can be achieved for a finite n , the capacity is said to be achievable non-asymptotically.

The communication complexity is the minimum public discussion rate required to achieve the secrecy capacity, i.e.,

$$R_S := \inf \limsup_{n \rightarrow \infty} \frac{1}{n} \log |F|, \quad (3.10)$$

where F denotes the finite alphabet set of possible values of F and the infimum is taken over all the discussion rates of C_S -achieving schemes.

Remark 3.1 Our problem formulation covers [1, 2] as special cases:

- Without silent active users, i.e., $S \subseteq D$, our formulation reduces to that in [1];
- Without trusted helpers, i.e., $A = V \setminus D$, but at least one vocal active user $A \setminus S \neq \emptyset$, we obtain the formulation in [2].

The wiretapper's side information in [1, 2] can be covered equivalently as the private source Z_i of a silent untrusted user $i \in S \cap D$. \square

We will focus on the case without silent untrusted users, i.e., $S \cap D = \emptyset$, because with silent untrusted users, even the secrecy capacity is largely unknown, let alone the communication complexity. Indeed, our case of interest will be further restricted to the following for a similar reason:

$S \subsetneq A$ with at least one vocal active user.

The secrecy capacity when all active users are silent remains unknown except in the special case with only two trusted users [21] or without helpers.² We also remark that certain user types need not be considered in the problem formulation.

Remark 3.2 Without loss of optimality, one *need not* consider the presence of the following users:

²In the case when all users are active and silent, i.e., $V = A = S$, it is straightforward to show that $C_S = J_{\text{GK}}(Z_V) := \max\{H(U) \mid H(U \mid Z_i) = 0, \forall i \in A\}$, which is the multivariate extension of Gács-Körner common information [22]. We want to point out that there is a subtle issue with our preliminary work in [17] that Gács-Körner common information was claimed but not proved to be the secrecy capacity at zero rate of public discussion. We are not able to extend the converse result [22] from no discussion to sub-linear amount (in n) of discussion. Hence, in [17], $C_S > J_{\text{GK}}(Z_V)$ can only be conjectured as a sufficient condition for $R_S > 0$.

- Untrusted active users, i.e., $A \not\subseteq V \setminus D$: The secrecy capacity is zero trivially because the recoverability condition (3.7) for such users means that the wiretapper can also recover the key, hence violating the secrecy condition (3.8).
- Silent trusted helpers, i.e., $S \not\subseteq A \cup D$: Their presence affect neither the recoverability condition (3.7) (by being silent) nor the secrecy condition 3.8 (by being trusted).

□

It was conjectured in [16] that private randomization does not reduce R_S in the case when all users are vocal and active. In the general case with helpers and silent users, the conjecture also appears very plausible, with no apparent counter-example that suggests otherwise. Indeed, as the following result shows, private randomization by any silent or untrusted user is not necessary, and so our formulation precluded them without loss of optimality.

Proposition 3.1 *Allowing private randomization by any silent or untrusted user $j \in S \cup D$, i.e., modifying (3.4) with*

$$\tilde{Z}_j = (U_j, Z_j^n) \quad \text{where } I(U_j \wedge \tilde{Z}_{V \setminus \{j\}}, Z_j^n) = 0 \quad (3.11)$$

neither increases C_S nor decreases R_S .

□

PROOF See Appendix A. ■

B. Optimality of Omniscience

Next, we take a step back to formulate the easier problem of the optimality of a general class of C_S -achieving strategies (in terms of minimizing the public discussion rate, i.e., achieving R_S). In both the case [1] (with helpers but no active users) and the case [2] (with active users but no helpers), it can be seen that the proposed C_S -achieving schemes require the active users to recover the private sources of the vocal users after public discussion. We will extend this idea to the following C_S -achieving scheme for the general case of interest described with helpers and silent users:

Definition 3.1 For $S \subsetneq A$, the *omniscience strategy for secret key agreement* requires each vocal user $i \in V \setminus S$ to broadcast in public a function³

$$F_i := f_i(\tilde{Z}_i) = f_i(Z_i^n) \quad (3.12)$$

of its source such that each active user can first recover the private sources of the (vocal) untrusted users in the sense that

$$\lim_{n \rightarrow \infty} \Pr(\exists i \in A, Z_D^n \neq \phi_i(Z_i^n, F_D)) = 0 \quad (3.13a)$$

for some function ϕ_i 's, and then recover the private sources of all other vocal users, i.e.,

$$\lim_{n \rightarrow \infty} \Pr(\exists i \in A, Z_{V \setminus D \setminus S}^n \neq \psi_i(\tilde{Z}_i, F_{V \setminus D \setminus S}, Z_D^n)) = 0 \quad (3.13b)$$

³Note that the omniscience strategy does not randomize (i.e., the U_i 's are deterministic in (3.3)).

for some function ψ_i 's. We also require the omniscience strategy to minimize the total discussion rate, denoted by

$$\begin{aligned} R_{CO} &:= \inf \limsup_{n \rightarrow \infty} \frac{1}{n} |F| \\ &= \inf \limsup_{n \rightarrow \infty} \frac{1}{n} \sum_{i \in V \setminus S} |F_i|, \end{aligned} \quad (3.14)$$

the infimum being taken over all functions f_i , $i \in V \setminus S$, that satisfy (3.12)–(3.13). The two recoverability constraints in (3.13) will be called the *omniscience constraints*, to distinguish them from the *recoverability constraint* (3.7) for the secret key. For the omniscience strategy to be C_S -achieving, we will also limit the discussion rates of the untrusted users to satisfy⁴

$$\left(\lim_{n \rightarrow \infty} \frac{1}{n} \log |F_i| \mid i \in D \right) \in \mathcal{R}(Z_D) \quad \text{where} \quad (3.15)$$

$$\mathcal{R}(Z_D) := \{r_D \in \mathbb{R}^D \mid r(B) \leq H(Z_B), \forall B \subseteq D\}. \quad (3.16)$$

The secret key is then chosen as a function

$$K = \theta(Z_{V \setminus S}^n) \quad (3.17)$$

of the entire private source of the vocal users at the maximum rate subject to the secrecy constraint (3.8). (Note that (3.7) immediately follows from (3.13).) □

We will show in Section V that the omniscience strategy is C_S -achieving in the general case of interest, and that R_{CO} has a single-letter linear-programming characterization. Therefore, R_{CO} serves as a computable upper bound on R_S . We say that omniscience is optimal for secret key agreement if the bound is tight, i.e., $R_S = R_{CO}$, in which case R_S has a single-letter characterization given by R_{CO} . Our goal is to discover general classes of scenarios under which omniscience is or is not optimal, i.e., the sufficient or necessary conditions for the optimality of omniscience. In particular, we will specialize/strengthen the results to the hypergraphical source model:

Definition 3.2 ([5, Definition 2.4]) Z_V is a hypergraphical source w.r.t. a hypergraph (V, E, ξ) with edge function $\xi : E \rightarrow 2^V \setminus \{\emptyset\}$ iff

$$Z_i = (X_e \mid e \in E, i \in \xi(e)) \quad \forall i \in V. \quad (3.18)$$

for some independent (hyper-)edge variables X_e for $e \in E$ with $H(X_e) > 0$. □

The above source model also covers the PIN model in [14, 15] as a special case:

Definition 3.3 ([15]) Z_V is a PIN iff it is hypergraphical w.r.t. a graph (V, E, ξ) with edge function $\xi : E \rightarrow V^2 \setminus \{(i, i) \mid i \in V\}$ (no self-loops). □

An example of a hypergraphical source and a PIN is given at the end of this section (Example 3.1).

⁴Although the proof of Theorem 5.1 relies on (3.15), we conjecture that (3.15) is not required for the omniscience strategy to be C_S -achieving.

We remark that the omniscience strategy above differs from that in [1] even in the case without silent users:

Remark 3.3 Instead of (3.13a), [1] require the entire source of the untrusted user to be revealed in public in the sense that

$$\lim_{n \rightarrow \infty} \Pr(Z_D^n \neq \phi(F_D)) = 0, \quad (3.19)$$

i.e., the source of the untrusted users can be recovered not only by the active users but also by anyone who gets to listen to the discussion F_D by the untrusted users. As will be shown by the following example, R_{CO} can be strictly larger with this requirement, resulting in a looser upper bound on R_S . The example also shows that (3.13a) and (3.13b) should not be combined into the constraint

$$\lim_{n \rightarrow \infty} \Pr(\exists i \in A, Z_{V \setminus S}^n \neq \phi_i(Z_i^n, F)) = 0 \quad (3.20)$$

because even an optimal discussion F under this constraint can leak too much information to the wiretapper. \square

Example 3.1 Let X_a and X_b be two uniformly random and independent bits, and

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= (X_a, X_b) \\ Z_3 &:= X_b \\ Z_4 &:= (X_a, X_b) \end{aligned}$$

With $V = [3]$, the source $Z_V = (Z_1, Z_2, Z_3)$ is a PIN with vertex set $[3]$, edge set $E = \{a, b\}$ and the edge function

$$\xi(e) = \begin{cases} \{1, 2\} & e = a \\ \{2, 3\} & e = b. \end{cases}$$

With $V = [4]$ instead, the source Z_V is not a PIN but a hypergraphical source with the edge function modified to

$$\xi(e) = \begin{cases} \{1, 2, 4\} & e = a \\ \{2, 3, 4\} & e = b. \end{cases}$$

Consider the scenario $(A, S, D, V) = (\{2, 4\}, \emptyset, \{3\}, [4])$. It can be shown that

$$C_S = 1 \quad \text{and} \quad R_S = R_{CO} = 0,$$

achieved non-asymptotically with

$$n = 1, \quad K := X_a \quad \text{and} \quad F \text{ deterministic.}$$

Hence, omniscience is optimal in this case. Now, if the recoverability condition (3.19) in [1] were imposed instead of (3.13a), then $R_{CO} \geq H(Z_3) = H(X_b) = 1 > 0 = R_S$, and so the omniscience scheme would not be optimal.

Consider the scenario $(A, S, D, V) = (\{1, 2, 4\}, \emptyset, \{3\}, [4])$ instead. It can be shown that

$$C_S = 1 \quad \text{and} \quad R_S = 0,$$

achieved non-asymptotically with

$$n = 1, \quad K = X_a \quad \text{and} \quad F \text{ deterministic.}$$

However, since the active user 1 does not observe X_b directly from its private source,

$$R_{CO} > H(Z_V|Z_1) \geq H(X_b) = 1,$$

which is achieved by choosing $F := F_3 := X_b$. It follows that $R_S = 0 < 1 = R_{CO}$, and so omniscience is not optimal. Now, if (3.20) were imposed instead of (3.13), then $R_{CO} = 1$ as before but it could be achieved with $F := F_2 := X_a \oplus X_b$, from which user 1 can recover X_b as $F \oplus Z_1$. However, the wiretapper can also recover Z_1 as $F \oplus Z_3$ by wiretapping the source of the untrusted user 3. Since the entire source, i.e., X_a and X_b , can be recovered by the wiretapper, any secret key K satisfying (3.17) and (3.8) must have zero rate. In other words, the current discussion for omniscience, despite being optimal in achieving R_{CO} , leaks too much information to the wiretapper. \square

IV. WITH NO HELPERS OR SILENT USERS

In this section, we will introduce the main ideas through the basic scenario $A = V$ and $S = \emptyset$. Unless stated otherwise, the basic scenario will be assumed for all the results in this section.

A. Preliminaries on MMI and Fundamental Partition

C_S in the current case is characterized by R_{CO} as:

Proposition 4.1 ([1]) *The omniscience strategy achieves*

$$C_S = H(Z_V) - R_{CO}, \quad (4.1)$$

and so $R_S \leq R_{CO}$. \square

R_{CO} was also characterized in [1] as a linear program using standard techniques of independent source coding [4]. The expression was argued to be solvable in polynomial time w.r.t. the size of the network [23, 24]. (This is assuming that the entropy function $B \mapsto H(Z_B)$ for $B \subseteq V$ can be evaluated in polynomial time.) Hence, R_{CO} may serve as an easily computable single-letter upper bound on R_S .

To study the tightness of the R_{CO} upper bound, we will make use of the following (conditional) multivariate mutual information (MMI) measure and its properties studied in [9]: For a finite set U and a random vector (Z'_U, W') ,

$$I(Z'_U|W') := \min_{\mathcal{P} \in \Pi'(U)} I_{\mathcal{P}}(Z'_U|W'), \quad \text{with} \quad (4.2a)$$

$$\begin{aligned} I_{\mathcal{P}}(Z'_U|W') &:= \frac{1}{|\mathcal{P}|-1} D \left(P_{Z'_U|W'} \left\| \prod_{C \in \mathcal{P}} P_{Z'_C|W'} \right\| P_{W'} \right) \\ &:= \frac{1}{|\mathcal{P}|-1} \left[\sum_{C \in \mathcal{P}} H(Z'_C|W') - H(Z'_U|W') \right], \end{aligned} \quad (4.2b)$$

where $\Pi'(U)$ is the collection of partitions of U into at least two non-empty disjoint parts, and $D(\cdot \| \cdot)$ is the conditional KL divergence. We also define the unconditional MMI measures $I(Z'_U)$ and $I_{\mathcal{P}}(Z'_U)$ by dropping the conditioning on W' throughout (4.2).

The MMI appeared as an upper bound on the secrecy capacity in [1, (26)] in the special case without helpers. In

[25], the bound [1, (26)] was shown to be loose in the more general case with helpers but identified to be tight in the no-helper case and therefore proposed as a measure of mutual information among multiple random variables:

Proposition 4.2 ([5, Theorem 1.1]) $C_S = I(Z_V)$ in the case without helpers or silent users. \square

The proof uses the submodularity [26] of the entropy function $B \mapsto H(Z'_B|W')$ for $B \subseteq U$ (a class of Shannon-type inequalities [27, 28]) to show that the linear-programming characterization of C_S in [1] is equal to the MMI. A simple proof using the Dilworth truncation was given in [9]. Like Shannon's mutual information, the MMI has various fundamental information-theoretic properties including the data processing inequality [9] (which will be refined in Lemma 6.1).

Denote the set of all optimal partitions to (4.2a) as

$$\Pi^*(Z'_U|W') := \{\mathcal{P} \in \Pi'(U) \mid I_{\mathcal{P}}(Z'_U|W') = I(Z'_U|W')\}. \quad (4.3)$$

The set $\Pi'(U)$ is endowed with a partial order, denoted by \preceq , with $\mathcal{P} \preceq \mathcal{P}'$ having the meaning

$$\forall C \in \mathcal{P}, \exists C' \in \mathcal{P}' \text{ such that } C \subseteq C'. \quad (4.4)$$

In other words, \mathcal{P} can be obtained from \mathcal{P}' by further partitioning some parts of \mathcal{P}' . We will consider the finest/smallest partition in $\Pi^*(Z'_U|W')$, the existence of which is guaranteed by the following proposition.

Proposition 4.3 ([9, Lemma 5.1 and Theorem 5.2])

$\Pi^*(Z'_U|W')$ forms a lower semi-lattice w.r.t. the partial order (4.4). In particular, there is a unique finest partition in $\Pi^*(Z'_U|W')$. \square

The unique finest partition in $\Pi^*(Z'_U|W')$ is called the *fundamental partition*, and is denoted as $\mathcal{P}^*(Z'_U|W')$. Again, the unconditional versions of these definitions, namely, $\Pi^*(Z'_U)$ and $\mathcal{P}^*(Z'_U)$, are obtained by dropping the conditioning on W' throughout. The fundamental partition has various meaningful interpretations in the problems of vocality [7, 8], successive omniscience [11], data clustering [29, 30] and feature selection [31].

The condition for the optimality of omniscience in [13, 16] for the PIN model in Definition 3.3 is expressed in terms of the fundamental partition.

Proposition 4.4 ([16, Theorem 8, Corollary 23]) For PIN, we have $R_S = R_{CO}$ iff $\mathcal{P}^*(Z_V) = \{\{i\} \mid i \in V\}$, namely, the partition into singletons. \square

The result was based on a lower bound on R_S in [16] that extends the result of [3] to the multiterminal setting using the multi-letter multivariate Wyner common information:

$$C_W := \inf \limsup_{n \rightarrow \infty} \frac{1}{n} H(L) \quad \text{such that} \quad (4.5a)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} I_{\mathcal{P}^*(Z_V)}(Z_V^n|L) = 0 \quad (4.5b)$$

where the infimum is for a given Z_V . Note that $\mathcal{P}^*(Z_V)$ is used instead of $\mathcal{P}^*(Z_V^n|L)$. Furthermore, [16] required L to be a function of \tilde{Z}_V , i.e., $H(L|\tilde{Z}_V) = 0$.

Proposition 4.5 ([16, Theorem 2]) The communication complexity R_S^{NR} with private randomization (3.3) precluded in the problem formulation is lowered bounded as

$$R_S^{\text{NR}} \geq C_W - I(Z_V), \quad (4.6)$$

which holds also with additional constraint that $H(L|\tilde{Z}_V) = 0$. \square

The use of the above lower bound is somewhat limited by the difficulty in evaluating the multi-letter expression C_W and the problem formulation that precludes randomization. The derivation of Proposition 4.4 requires quite a bit of machinery to evaluate C_W , and to extend the result to allow randomization. We will improve the bound (in Theorem 4.1 in Section IV-B) with a single-letter expression:

Definition 4.1 For a finite set U with size $|U| > 1$ and random vector (Z'_U, W') , the (conditional) *partition Wyner common information* of Z'_U given W' w.r.t. the partition $\mathcal{P} \in \Pi'(U)$ is

$$J_{W, \mathcal{P}}(Z'_U|W') := \inf \{I(W \wedge Z'_U|W') \mid \quad (4.7a)$$

$$I_{\mathcal{P}}(Z'_U|W, W') = 0\}, \quad (4.7b)$$

where the minimum is taken over all possible choices of the random variable W (or $P_{W|Z'_U, W'}$). $J_W(Z'_i \wedge Z'_j|W')$ denotes the bivariate case $U = \{i, j\}$ where $i \neq j$. (The version without conditioning reduces to the usual Wyner common information introduced by [32].) \square

If \mathcal{P} is the partition into singletons, and W' is deterministic, then $J_{W, \mathcal{P}}$ is the extension in [33] of the Wyner common information [32] from the bivariate case $J_W(Z_i \wedge Z_j)$, to the multivariate case. Following the same argument as in [32], the expression (4.7) is computable with the following bound on support size:

Proposition 4.6 For the partition Wyner common information (4.7), it is admissible to impose

$$|W| \leq |Z'_U||W'|, \quad (4.8)$$

and \inf can be replaced by \min , i.e., the infimum can be achieved by a choice of W satisfying (4.8) in addition. \square

PROOF This follows from the same argument as in [32] and will be proved for the more general setting in Proposition 6.3. \blacksquare

Despite the above result, $J_{W, \mathcal{P}}$ is not easy to compute even for the bivariate case [32]. Fortunately, it has non-trivial entropic [9] bounds that are easy to compute from the entropy function of the given random vector:

Proposition 4.7

$$H(Z'_U|W') \geq J_{W, \mathcal{P}}(Z'_U|W') \geq J_{D, \mathcal{P}}(Z'_U|W') \quad \text{where} \quad (4.9)$$

$$J_{D, \mathcal{P}}(Z'_U|W') := H(Z'_U|W') - \sum_{C \in \mathcal{P}} H(Z'_C|Z'_{U \setminus C}, W'), \quad (4.10)$$

which will be called the partition dual total correlation. \square

PROOF Since $W = Z'_U$ is always a feasible solution to (4.7), $J_{W,\mathcal{P}}(Z'_U|W') \leq H(Z'_U|W')$, which gives the first inequality in (4.9). To prove the second inequality, it suffices to show

$$I(W \wedge Z'_U|W') \geq J_{D,\mathcal{P}}(Z'_U|W')$$

for all feasible solution W . To do so, notice that the constraint (4.7b) means that Z_C for $C \in \mathcal{P}$ are mutually independent given (W, W') , and so

$$\begin{aligned} I(W \wedge Z'_U|W') &= H(Z'_U|W') - H(Z'_U|W', W) \\ &\stackrel{(a)}{=} H(Z'_U|W') - \sum_{C \in \mathcal{P}} H(Z'_C|W', W) \\ &\stackrel{(b)}{=} H(Z'_U|W') - \sum_{C \in \mathcal{P}} H(Z'_C|W', W, Z'_{U \setminus C}) \\ &\geq H(Z'_U|W') - \sum_{C \in \mathcal{P}} H(Z'_C|W', Z'_{U \setminus C}) \\ &= J_{D,\mathcal{P}}(Z'_U|W'), \end{aligned}$$

where we have applied the independence of Z_C 's in (a) and (b) to rewrite to rewrite $H(Z'_U|W, W')$ as the sum $\sum_{C \in \mathcal{P}} H(Z'_C|W', W, Z'_{U \setminus C})$. \blacksquare

When \mathcal{P} is the partition into singletons, $J_{D,\mathcal{P}}$ is Han's dual total correlation [34], and was shown to be the best entropic lower bound for $J_{W,\mathcal{P}}$ even after incorporating non-Shannon-type inequalities [35].

B. Main results

We give a single-letter lower bound on R_S that improves upon the result of Proposition 4.5 by allowing private randomization.

Theorem 4.1 For any source Z_V ,

$$R_S \geq J_{W,\mathcal{P}^*}(Z_V) - I(Z_V) \quad (4.11a)$$

$$\geq J_{D,\mathcal{P}^*}(Z_V) - I(Z_V) \quad (4.11b)$$

where \mathcal{P}^* denotes $\mathcal{P}^*(Z_V)$ for convenience, and J_{W,\mathcal{P}^*} and J_{D,\mathcal{P}^*} are the partition Wyner common information (4.7) and the partition dual total correlation (4.10). \square

PROOF See Appendix B-1. \blacksquare

It was shown in [9] that $J_{D,\mathcal{P}^*}(Z_V)$ is no smaller than $I(Z_V)$, therefore, the lower bounds above are non-negative.

Corollary 4.1 $R_S = R_{CO}$ if $J_{W,\mathcal{P}^*}(Z_V) = H(Z_V)$.

PROOF This follows from Theorem 4.1 by virtue of Proposition 4.1 and 4.2, i.e., substituting $J_{W,\mathcal{P}^*}(Z_V) = H(Z_V)$ and $I(Z_V) = C_S$ to the r.h.s. of (4.11a) gives R_{CO} . \blacksquare

Compared to Proposition 4.4, (4.11a) is single-letter rather than multi-letter. Furthermore, (4.11b) is a simple linear function of the entropy vector of Z_V given $\mathcal{P}^*(Z_V)$, which is easier to evaluate than (4.11a).

From Corollary 4.1, we obtain the following sufficient condition for the optimality of omniscience under a general source model:

Theorem 4.2 $R_S = R_{CO}$ if

$$H(Z_C|Z_{V \setminus C}) = 0 \quad \forall C \in \mathcal{P}^*(Z_V), \quad (4.12)$$

where \mathcal{P}^* is the fundamental partition in Proposition 4.3, namely, the finest optimal partition for the MMI (4.2a). \square

PROOF The condition in (4.12) implies that $J_{D,\mathcal{P}^*}(Z_V) = H(Z_V)$, and therefore, by (4.9), we also have $J_{W,\mathcal{P}^*}(Z_V) = H(Z_V)$. The theorem now follows from Corollary 4.1. \blacksquare

Condition (4.12) means that, for all $C \in \mathcal{P}^*(Z_V)$, no randomness of Z_C is independent of $Z_{V \setminus C}$, i.e., specific to Z_C . This condition covers all the existing results:

- (4.12) covers the condition for the 2-user case in Proposition 2.1 because $\mathcal{P}^*(Z_{\{1,2\}}) = \{\{1\}, \{2\}\}$.
- (4.12) also extends the sufficiency part of the condition in Proposition 4.4 because (4.12) holds for $\mathcal{P}^*(Z_V) = \{\{i\} : i \in V\}$ trivially, as every edge variable X_e ($e \in E$) is a component of Z_j and Z_k for the distinct pair $\{j, k\} = \xi(e)$ of incident nodes.

Despite its generality, (4.12) can be checked easily because $\mathcal{P}^*(Z_V)$ can be computed in strongly polynomial-time. The following is an example for which the optimality of omniscience can be easily derived by (4.12) but not by the existing results.

Example 4.1 (4.12) holds for the source in Example 2.2 as

$$\begin{aligned} \mathcal{P}^*(Z_{\{1,2,3\}}) &= \{\{1\}, \{2\}, \{3\}\}, \quad \text{and} \\ H(Z_1|Z_2, Z_3) &= H(Z_2|Z_1, Z_3) = H(Z_3|Z_1, Z_2) = 0. \end{aligned}$$

Hence, $R_S = R_{CO}$ by Theorem 4.2. This example is not covered by Proposition 4.4 because the private source belongs to the more general finite linear source model [12] rather than the PIN model (Definition 3.3) (or the hypergraphical source model in Definition 3.2). \square

C. Stronger Results for Hypergraphical Sources

The necessity of the condition in Proposition 4.4 can be extended to the more general hypergraphical source model in Definition 3.2:

Theorem 4.3 For hypergraphical sources w.r.t. the hypergraph (V, E, ξ) , we have $R_S = R_{CO}$ iff

$$\nexists e \in E, C \in \mathcal{P}^*(Z_V) : \xi(e) \subseteq C, \quad (4.13)$$

i.e., every hyperedge crosses the fundamental partition. \square

PROOF See Section B-2. \blacksquare

Example 4.2 Let X_a, X_b and X_c be uniformly random and independent bits. With $V := [5]$, define the private source as

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= X_b \\ Z_3 &:= X_c \\ Z_4 &:= (X_a, X_b) \\ Z_5 &:= (X_a, X_b, X_c). \end{aligned}$$

It is hypergraphical with edge function

$$\xi(e) = \begin{cases} \{1, 4, 5\} & e = a \\ \{2, 4, 5\} & e = b \\ \{3, 5\} & e = c. \end{cases}$$

To check condition (4.13), we can first obtain

$$I(Z_V) = 1 \quad \text{and} \quad \mathcal{P}^*(Z_V) = \{\{1\}, \{2\}, \{3\}, \{4, 5\}\}.$$

Then, (4.13) holds because every hyperedge crosses $\mathcal{P}^*(Z_V)$. (4.12) also holds because, for every $C \in \mathcal{P}^*(Z_V)$, every edge variable in Z_C also appears in $Z_{V \setminus C}$. By Theorem 4.2,

$$R_S = R_{CO} = H(Z_V) - I(Z_V) = 2 \quad \text{by (4.1)}.$$

This can be achieved non-asymptotically with $n = 1$, $K := Z_1 = X_a$ and $F_5 := (X_a \oplus X_b, X_a \oplus X_c)$. \square

$J_{W, \mathcal{P}^*}(Z_V)$ can be evaluated for hypergraphical sources because its lower bound by (4.9) is tight:

Proposition 4.8 For hypergraphical sources w.r.t. the hypergraph (V, E, ξ) , we have

$$J_{W, \mathcal{P}^*}(Z_V) = H(X_{E^*}) \quad \text{where} \quad (4.14a)$$

$$E^* := \{e \in E \mid \exists C \in \mathcal{P}^*(Z_V), \xi(e) \subseteq C\} \quad (4.14b)$$

is the set of hyperedges that cross $\mathcal{P}^*(Z_V)$. Furthermore, an optimal solution to (4.7) is $W := (X_e \mid e \in E^*)$. \square

PROOF See Appendix B-3. \blacksquare

This means that the lower bound (4.11a) can be easily computed for hypergraphical sources. Interestingly, while the lower bound leads to a complete characterization of the optimality of omniscience for the hypergraphical model, it may be loose for the PIN model when condition (4.13) is not satisfied, as shown by the example below.

Example 4.3 Let X_a, X_b and X_c be uniformly random and independent bits. With $V = [3]$, define

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= (X_a, X_b, X_c) \\ Z_3 &:= (X_b, X_c), \end{aligned} \quad (4.15)$$

which is a PIN. It can be shown that

$$I(Z_V) = 1 \quad \text{and} \quad \mathcal{P}^*(Z_V) = \{\{1\}, \{2, 3\}\}.$$

The edge a is the only edge that crosses $\mathcal{P}^*(Z_V)$. Therefore, $J_{W, \mathcal{P}^*}(Z_V) = H(X_a) = 1$, and so (4.11a) gives the trivial lower bound $R_S \geq 1 - 1 = 0$. However, it was proved in [36] that $R_S = 1$ for this example, and so the bound is loose. \square

V. SINGLE-LETTER UPPER BOUNDS AND NECESSARY CONDITIONS

In this section, we consider the general case $S \subsetneq A$, with possibly helpers and silent users. The single-letter upper bound on R_S by R_{CO} continues to hold in the more general case because the omniscience strategy in Definition 3.1 can be shown to be C_S -achieving.

A. Smallest Rate of CO

The following result establishes the R_{CO} upper bound on R_S and characterizes C_S and R_{CO} .

Theorem 5.1 With $S \subsetneq A$, the omniscience strategy in Definition 3.1 is C_S -achieving, with

$$C_S = H(Z_{V \setminus D \setminus S} \mid Z_D) - \rho \quad (5.1)$$

$$R_S \leq R_{CO} = \bar{\rho} + \rho \quad (5.2)$$

where ρ and $\bar{\rho}$ are defined as the following linear programs:

$$\rho := \min \{r(V \setminus D \setminus S) \mid r_{V \setminus D \setminus S} \in \mathbb{R}^{V \setminus D \setminus S}, \quad (5.3a)$$

$$r(B) \geq H(Z_B \mid Z_{V \setminus S \setminus B}, Z_j) \quad \forall j \in A, B \subseteq V \setminus D \setminus S\} \quad (5.3b)$$

$$\bar{\rho} := \min \{r(D) \mid r_D \in \mathcal{R}(Z_D), \quad (5.4a)$$

$$r(B) \geq H(Z_B \mid Z_{D \setminus B}, Z_j) \quad \forall j \in A, B \subseteq D\}. \quad (5.4b)$$

$\mathcal{R}(Z_D)$ is defined in (3.16), and we have used the notation $r_B := (r_i \mid i \in B)$ and $r(B) := \sum_{i \in B} r_i$ for any set B . \square

PROOF See Appendix C-1. \blacksquare

The single-letter characterizations for ρ and $\bar{\rho}$ in (5.3) and (5.4) can be computed in polynomial time,⁵ and hence, so can C_S and R_{CO} . (5.1) covers the results of [1, 2] as the following special cases:

Corollary 5.1 ([1, Theorem 2]) For $S = \emptyset$,

$$C_S = H(Z_{V \setminus D} \mid Z_D) - \rho \quad \text{where}$$

$$\rho = \min \{r(V \setminus D) \mid r(B) \geq H(Z_B \mid Z_{V \setminus B}), \forall B \in \mathcal{H}\}$$

and $\mathcal{H} := \{B \subseteq V \setminus D \mid \emptyset \neq B \not\subseteq A\}$. \square

PROOF When $S = \emptyset$, (5.3b) becomes

$$r(B) \geq H(Z_B \mid Z_{V \setminus B}, Z_j), \forall j \in A, B \subseteq V \setminus D.$$

This yields the expression in the corollary after removing the redundant constraints where $B = \emptyset$ or $B \ni j$. \blacksquare

Corollary 5.2 ([2, Theorem 6]) For $S \subsetneq A = V$,

$$C_S = H(Z_{V \setminus S}) - \rho \quad \text{where}$$

$$\rho = \min \{r(V \setminus S) \mid r(B \setminus S) \geq H(Z_{B \setminus S} \mid Z_{V \setminus B}), \forall B \in \mathcal{H}\}$$

and $\mathcal{H} := \{B \subseteq V \mid \emptyset \neq B \not\subseteq A\}$. \square

PROOF With $S \subsetneq A = V$, (5.3b) becomes

$$r(B) \geq H(Z_B \mid Z_{V \setminus S \setminus B}, Z_j) \quad \forall j \in A, B \subseteq V \setminus S.$$

⁵This can be argued as in [23] by noting that the separation oracle corresponds to performing a polynomial number of submodular function minimizations, which can be done in polynomial time.

The constraints with $B \ni j$ are again redundant and so we can impose $j \notin B$. With $B' = B \cup S \setminus \{j\}$, the constraints can be rewritten as

$$r(B' \setminus S) \geq H(Z_{B' \setminus S} | Z_{V \setminus B'}).$$

The constraints can only be weaker if some element in S is removed from B' , as the r.h.s. cannot increase but the l.h.s. remains unchanged. This yields the expression in the corollary. ■

As illustrated by Example 3.1, $\bar{\rho}$ can be strictly smaller than $H(Z_D)$, i.e., the omniscience strategy is an improved version of that [1] when $S = \emptyset \neq D$. Consequently, the R_{CO} upper bound (5.2) is also improved.

B. Change of Scenario

In this section we will introduce some general techniques to strengthen the upper bound on R_S . In particular, we will make use of the monotonicity of (C_S, R_S) w.r.t. certain changes of scenario, namely the vector (A, S, D, V, Z_V) of user sets and the private source. We first consider changes in the user sets.

Theorem 5.2 Suppose (C_S, R_S) becomes (C'_S, R'_S) by one of the following changes in the user sets:

- (i) A vocal active user is turned into a silent active user, and a new trusted helper with the same private source as the original vocal active user is added. That is to say, (S, V) becomes $(S \cup \{i\}, V \cup \{i'\})$ for some $i \in A \setminus S$, with $i' \notin V$ being a new user with private source $Z_{i'} = Z_i$.
- (ii) A trusted helper is removed, i.e., V becomes $V \setminus \{i\}$ for some $i \in V \setminus (A \cup D)$.

Then, we have $C'_S \leq C_S$. If equality holds, then $R'_S \geq R_S$. □

PROOF See Appendix C-2. ■

Therefore, using Theorem 5.2, if $C'_S = C_S$, then the R_{CO} of the new scenario can serve as an upper bound on the R_S of the original scenario. This leads to the following application.

Corollary 5.3 With $S \subsetneq A$, if C_S remains unchanged after

- (i) turning a proper subset of vocal active users into silent active users, and
 - (ii) removing all the trusted helpers,
- i.e., (S, V) becomes (S', V') causing (C_S, R_S, R_{CO}) to change to (C'_S, R'_S, R'_{CO}) , such that $C_S = C'_S$, $V' = A \cup D$, $S \subseteq S' \subsetneq A$. Then,

$$R_S \leq R'_S \leq R'_{CO} \leq R_{CO}. \quad (5.5)$$

It follows that $R_S = R_{CO}$ only if $C_S \neq C'_S$ or

$$H(Z_{V' \setminus S'}) = H(Z_{V \setminus S}), \quad (5.6)$$

i.e., $H(Z_{(S' \setminus S) \cup (V \setminus V')}) = 0$. □

PROOF See Appendix C-2. ■

The following is another application of Theorem 5.2 when the entire set of vocal active users is turned into silent active users.

Corollary 5.4 With $S \subsetneq A$, if

$$C_S \leq H(U|Z_D) \quad (5.7)$$

for any common function U such that

$$H(U|Z_i) = 0 \quad \forall i \in A, \quad (5.8)$$

then $R_S = 0$. In this case, $R_S = R_{CO}$ iff $R_{CO} = 0$, i.e.,

$$H(Z_{V \setminus S} | Z_i) = 0, \quad \forall i \in A. \quad (5.9)$$

PROOF See Appendix C-2. ■

Example 5.1 To illustrate Corollary 5.3, consider Example 2.1 with $A = V = \{1, 2\}$, $D = S = \emptyset$, $Z_1 = (X_0, X_1)$ and $Z_2 = (X_J, J)$. If we choose $S' = \{1\}$ and everything else the same, then condition (5.6) fails because $H(Z_2) = 2 < 3 = H(Z_{\{1, 2\}})$, or equivalently, $H(Z_1 | Z_2) = 1 > 0$, but $C'_S = I(Z_1 \wedge Z_2) = C_S$, which follows from Proposition 6.4 and (4.2). Hence, by Corollary 5.3, $R_S < R_{CO}$ as expected. □

Example 5.2 The necessary condition (5.6) may not be sufficient in general. For instance, consider Example 4.3 with $A = V = [3]$ but with $S = \{1, 3\}$. Note that the only possible choice of S' in (5.6) is S , and so (5.6) holds trivially. However, by result of [37], it can be shown that the randomness of X_c can be reduced without diminishing the capacity. In this example, $C_S = \min\{I(Z_1 \wedge Z_2), I(Z_2 \wedge Z_3)\} = 1$ by Proposition 6.4, which remains unchanged even if X_c is eliminated (doing so will only reduce $I(Z_2 \wedge Z_1)$ from 2 to 1). Consequently, $R'_{CO} < R_{CO}$, and hence, $R_S \leq R'_S < R_{CO}$. □

The following is a single-letter bound that generalizes the idea beyond the hypergraphical source.

Theorem 5.3 For any finite set Q , let

$$Z_i^{(q)} := \zeta_i^{(q)}(Z_i) \quad \forall i \in V, q \in Q, \quad (5.10)$$

and for some functions $\zeta_i^{(q)}$ such that

$$I(Z_{V \setminus D}^{(q)} \wedge Z_D | Z_D^{(q)}) = 0 \quad \forall q \in Q. \quad (5.11)$$

If, for some random variable Q independent of Z_V , we have

$$C_S \leq H(Z_{V \setminus S}^{(Q)} | Q) - R'_{CO}, \quad (5.12)$$

where R'_{CO} is the smallest rate of CO for $Z_V^{(Q)}$ given Q (i.e., with Q observed a priori), then

$$R_S \leq R'_{CO} \leq H(Z_{V \setminus S}^{(Q)} | Q) - C_S. \quad (5.13)$$

PROOF See Appendix C-3. ■

This result covers the PIN model in Example 5.2, with Q chosen to be deterministic and Z_V processed to Z'_V , where $Z'_1 := Z_1 = X_a$, $Z'_2 := (X_a, X_b)$, $Z'_3 := X_b$. The following example shows that (5.11) is useful in handling the case with untrusted helpers as well.

Example 5.3 Consider the same source as in Example 5.2 (Example 4.3) but with $(A, S, D) = (\{2, 3\}, \emptyset, \{1\})$ instead. Then, $C_S = I(Z_2 \wedge Z_3 | Z_1) = 2$. We process Z_V to Z'_V where $Z'_2 = Z_2 = (X_b, X_c)$, $Z'_3 = (X_b, X_c)$, and Z'_1 is deterministic. Then, the secrecy capacity remains unchanged, i.e., equal to $I(Z'_2 \wedge Z'_3 | Z'_1) = 2$, and $I(Z'_{V \setminus D} \wedge Z_D | Z'_D) = I(Z'_{\{2,3\}} \wedge Z_1) = I(X_b, X_c \wedge X_a) = 0$ satisfy (5.11). $R'_{CO} = 0$ since $Z'_{\{1,2,3\}} = Z'_2 = Z'_3$, and so $R_S = 0 < R_{CO} = H(Z_1) = 1$ by Theorem 5.3, and so, omniscience is not optimal. \square

Note that, in the above example, the edge variable X_c observed by the untrusted user 3 can be removed without affecting R_S . This can be proved more generally:

Proposition 5.1 For any random variable X independent of Z_V , consider the new scenario with Z_V changed to Z'_V where

$$Z'_i = \begin{cases} (Z_i, X) & i \in T \\ Z_i & \text{otherwise,} \end{cases} \quad (5.14)$$

for some $T \subseteq V$ such that $T \cap D \neq \emptyset$, i.e., X is observed by the wiretapper. Then, both C_S and R_S remain unchanged. \square

PROOF To prove Proposition 5.1, note that the proof of Proposition 3.1 in Appendix A remains valid even if \tilde{U}_i for an untrusted user $i \in D$ is observed by other user $j \in V$, i.e., with (3.5) modified to have F_i depend on \tilde{U}_i directly. Hence, with $\tilde{U}_i = X^n$, the proof of Proposition 3.1 shows that X^n neither increases C_S nor decreases R_S , as desired. \blacksquare

Corollary 5.5 For any hypergraphical source, the hyperedges $e \in E$ with $\xi(e) \cap D \neq \emptyset$ can be removed without changing C_S and R_S . \square

PROOF The corollary follows from Proposition 5.1 with Z'_V being the original hypergraphical source and Z_V being the source after removing the edge variable $X := X_e$. \blacksquare

While Q was chosen to be deterministic for the previous example, it is sometimes useful to make Q random as shown by the following example.

Example 5.4 Let X_a, X_b, X_c, X_d and X_e be uniformly random and independent bits, and define

$$\begin{aligned} Z_1 &:= (X_a, X_b, X_e) \\ Z_2 &:= (X_a, X_b, X_c) \\ Z_3 &:= (X_c, X_d) \\ Z_4 &:= (X_d, X_e) \end{aligned}$$

With $A = V = [4], S = D = \emptyset$, we have

$$\begin{aligned} C_S &= I(Z_V) = 1.5 \quad \text{with} \\ P^*(V) &= \{\{1, 2\}, \{3\}, \{4\}\} \\ R_{CO} &= H(Z_V) - I(Z_V) \\ &= 5 - 1.5 = 3.5. \end{aligned}$$

Let Q be a uniformly random bit independent of Z_V and process Z_V to $Z_V^{(Q)}$ with $Z_i^{(Q)} := Z_i$ for $i \in \{2, 3\}$ but

$$\begin{aligned} Z_1^{(Q)} &:= \begin{cases} (X_a, X_b, X_e) & \text{if } Q = 1 \\ (X_a, X_b) & \text{otherwise, and} \end{cases} \\ Z_4^{(Q)} &:= \begin{cases} (X_d, X_e) & \text{if } Q = 1 \\ X_d & \text{otherwise.} \end{cases} \end{aligned}$$

It follows that

$$\begin{aligned} H(Z_{\{1,4\}}^{(Q)} | Q) &= 0.5H(X_{\{a,b,d,e\}}) + 0.5H(X_{\{a,b,d\}}) \\ &= 3.5 < 4 = H(Z_{\{1,4\}}). \end{aligned}$$

By Proposition 4.1 and 4.2, we have $R'_{CO} = H(Z_V^{(Q)} | Q) - I(Z_V^{(Q)} | Q) = 4.5 - 1.5 = 3$, because

$$\begin{aligned} H(Z_V^{(Q)} | Q) &= \frac{4 + 5}{2} = 4.5 \quad \text{and} \\ I(Z_V^{(Q)} | Q) &= \frac{2.5 + 2.5 + 2 + 2 - 4.5}{3} = 1.5. \end{aligned}$$

Hence, $R_S \leq R'_{CO} < R_{CO}$, and so omniscience is not optimal.

It can be seen the benefit of making Q random is that it allows the edge e to be removed a fraction (half) of the time. Note that a complete removal of the edge, i.e., with $Q = 0$ deterministically, is suboptimal, because it diminishes the secrecy capacity, i.e.,

$$I(Z_V^{(Q)} | Q = 0) = \frac{2 + 2 + 2 + 2 - 4}{3} = \frac{4}{3} < 1.5. \square$$

The following example shows that Theorem 5.3 is useful for more general sources that are not necessarily hypergraphical.

Example 5.5 Let X_0, X_1 and J be uniformly random and independent bits, and define

$$\begin{aligned} Z_1 &:= (J, X_0 \oplus X_1) \\ Z_2 &:= (X_0, X_1) \\ Z_3 &:= X_J. \end{aligned}$$

With $A = V = [3]$ and $S = D = \emptyset$, we have $C_S = I(Z_V) = 1$ and $R_{CO} = H(Z_V) - I(Z_V) = 2$. Now, with $Z'_i := Z_i$ for $i \in \{2, 3\}$ and

$$Z'_1 := \begin{cases} (J, X_0 \oplus X_1) & \text{if } X_0 \neq X_1, \text{ i.e., } X_0 \oplus X_1 = 1, \\ X_0 \oplus X_1 & \text{otherwise,} \end{cases}$$

(or, alternatively, $Z'_1 := (2J - 1) \cdot (X_0 \oplus X_1)$ which takes value from $\{-1, 0, 1\}$.) It follows that

$$\begin{aligned} H(Z'_1) &\stackrel{(a)}{=} H(X_0 \oplus X_1, Z'_1) \\ &= H(X_0 \oplus X_1) + H(Z'_1 | X_0 \oplus X_1) \\ &\stackrel{(b)}{=} 1 + 0.5 = 1.5 < 2 = H(Z_1) \end{aligned}$$

where (a) is because Z'_1 determines $X_0 \oplus X_1$; (b) is because $H(Z'_1 | X_0 \oplus X_1 = 0) = 0$ while $H(Z'_1 | X_0 \oplus X_1 = 1) = H(J) = 1$. Using this, it can be shown that (C'_S, R'_{CO}) is given by $C'_S = I(Z'_V) = 1$ and $R'_{CO} = H(Z'_V) - I(Z'_V) = 2.5 - 1 = 1.5$. By Theorem 5.3, we have $R_S \leq R'_{CO} < R_{CO}$, and so the

omniscience strategy is not optimal. Indeed, it can be shown that $R_S = 1.5$ by the result of [36].

As an interesting side note, although the omniscience strategy is not optimal, it can be non-asymptotic, for instance, by setting $n = 1$, $K = X_J$, $F_1 = J$, $F_2 = X_{1-J}$ and F_3 deterministic. However, it seems impossible to achieve $R_S \leq 1.5$ non-asymptotically. To construct an asymptotic scheme, note that the fraction of time $X_0 \oplus X_1 = 0$ is $1/2$ almost surely as $n \rightarrow \infty$ by the law of large number. Whenever $X_0 \oplus X_1 = 0$, both user 1 and 2 knows. In particular, user 2 can recover X_{1-J} even without knowing J since $X_0 = X_1$. Hence, X_J can potentially be used as a secret key bit without omniscience of the source, i.e., without user 2 knowing J all the time. To do so, however, the public discussion must be chosen carefully in order not to let the wiretapper know the time instances when $X_0 = X_1$. This can be done by an asymptotic scheme, where the realizations of J for the time instances when $X_0 \neq X_1$ are concatenated and then truncated/zero-padded by user 1 to form a sequence of length $n/2 + \sqrt{n}$. Then, the sequence can be revealed in public as F_1 , which does not leak any information about the time instances where $X_0 = X_1$. Since user 2 can recover $X_0 \oplus X_1$ from his private observation, he can recover the sequence of realizations of Z_{J-1} almost completely (close to a fraction of 1 by the law of large number) and reveal it in public as F_2 . Hence, almost the entire sequence of X_J can be recovered by everyone and used as the secret key. \square

VI. SINGLE-LETTER LOWER BOUNDS AND SUFFICIENT CONDITIONS

In this section, we derive general single-letter bounds on R_S . We will first extend the definitions in (4.2) to characterize C_S .

A. Fractional Partition Information

We will use the following generalization of the notion of partitions. For a finite set U , a *fractional partition* is a non-negative set function $\lambda : 2^U \rightarrow \mathbb{R}_+$ that satisfies

$$\sum_{B \subseteq U: i \in B} \lambda(B) = 1 \quad \forall i \in U. \quad (6.1)$$

For a set family $\mathcal{H} \subseteq 2^U \setminus \{\emptyset\}$, we use $\Lambda(U, \mathcal{H})$ to denote the set of fractional partitions λ whose support lies within \mathcal{H} , i.e.,

$$\text{supp}(\lambda) := \{B \subseteq U \mid \lambda(B) > 0\} \subseteq \mathcal{H}. \quad (6.2)$$

For instance, the indicator function $\chi_{\mathcal{P}}$ of a partition $\mathcal{P} \in \Pi(U)$ is a fractional partition, i.e.,

$$\lambda(B) = \chi_{\mathcal{P}}(B) = \begin{cases} 1 & B \in \mathcal{P} \\ 0 & \text{otherwise.} \end{cases} \quad (6.3)$$

However, the notion of fractional partition is more general. An important case of interest is

$$\lambda(C) = \frac{\chi_{\mathcal{P}}(U \setminus C)}{|\mathcal{P}| - 1} = \begin{cases} \frac{1}{|\mathcal{P}| - 1} & U \setminus C \in \mathcal{P} \\ 0 & \text{otherwise,} \end{cases} \quad (6.4)$$

for some $\mathcal{P} \in \Pi'(U)$. This is called a *co-partition*.

Definition 6.1 ([9, (4.4b)]) For a finite set U with size $|U| > 1$, $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$ and a random vector (Z'_U, W') , define the (conditional) *fractional partition information* as

$$I_{\lambda}(Z'_U|W') := H(Z'_U|W') - \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) H(Z'_B|Z'_{U \setminus B}, W'). \quad (6.5)$$

For $\mathcal{P} \in \Pi'(U)$, $I_{\mathcal{P}}(Z'_U|W')$ (4.2b) and $J_{D, \mathcal{P}}(Z'_V|W')$ (4.10) are the special cases of $I_{\lambda}(Z'_U|W')$ when λ satisfies (6.4) and (6.3) respectively. \square

The secrecy capacity in the case without silent users can be characterized by I_{λ} as follows:

Proposition 6.1 ([38, Theorem 3.1]) For $S = \emptyset$,

$$C_S = \min_{\lambda \in \Lambda(V \setminus D, \mathcal{H})} I_{\lambda}(Z_{V \setminus D}|Z_D) \quad (6.6)$$

where $\mathcal{H} := \{B \subseteq V \setminus D : \emptyset \neq B \not\supseteq A\}$. \square

Like $I_{\mathcal{P}}(Z_V)$ (4.2b), $I_{\lambda}(Z'_V)$ (6.5) is also non-negative [38], which is a consequence of the Shearer-type lemma in [39]. We will need the stronger statement below (with an equality condition):

Proposition 6.2 ([9, Lemma 6.1]) For any random vector (Z'_U, W') and $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$, we have $I_{\lambda}(Z'_U|W') \geq 0$ with equality iff

$$I(Z'_B \wedge Z'_{U \setminus B}|W') = 0 \quad \forall B \in \text{supp}(\lambda), \quad (6.7)$$

which is the condition in terms of Shannon's mutual information for the fractional partition information to be zero. \square

For completeness, we will prove a stronger version of the result in Appendix D-1.

As pointed out in [9, Footnote 17], I_{λ} (6.5) also satisfies the data processing inequality [9, (5.20b)]. We will use the following more elaborate version:

Lemma 6.1 For any random vector (Z'_U, W', Y') , $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$ and $i \in U$, we have

$$I_{\lambda}(Z'_U|W') \geq I_{\lambda}(Z''_U|W') - \delta, \quad (6.8)$$

where

$$Z''_j := \begin{cases} Y', & j = i \\ Z'_j, & j \in U \setminus \{i\} \end{cases} \quad \text{and} \quad \delta := \left(\sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) - 1 \right) I(Y' \wedge Z'_{U \setminus \{i\}}|W', Z'_i).$$

Furthermore,

$$I_{\lambda}(Z'_U|W') \geq I_{\lambda}(Z'_U|W', Y') - \delta + \gamma, \quad (6.9)$$

where

$$\gamma := \min_{\substack{B \in \text{supp}(\lambda): \\ i \in B}} \max_{j \in U \setminus B} I(Y' \wedge Z'_j|W')$$

and δ is as defined for (6.8). \square

PROOF See Appendix D-2. \blacksquare

(6.8) and (6.9) can be viewed as the extensions of the following well-known data processing inequality in the bivariate case $U = \{1, 2\}$ for the Markov chain $Z'_1 - Z'_2 - Y'$ (i.e., $I(Z'_1 \wedge Y' | Z'_2) = 0$):

$$I(Z'_1 \wedge Z'_2) \geq I(Z'_1 \wedge Y') \quad \text{and} \quad (6.10a)$$

$$I(Z'_1 \wedge Z'_2) \geq I(Z'_1 \wedge Z'_2 | Y') + I(Z'_1 \wedge Y'). \quad (6.10b)$$

More precisely, $\Lambda(U, 2^U \setminus \{\emptyset, U\})$ contains only the partition (co-partition) λ with $\lambda(\{1\}) = \lambda(\{2\}) = 1$. With $i = 2$ and $W' = \emptyset$, (6.8) reduces to (6.10a), while (6.9) reduces to (6.10b).

B. General lower bound

The lower bound on R_S will be stated and derived using the following single-letter expression that extends the partition Wyner common information (4.7):

Definition 6.2 For a finite set U with size $|U| > 1$, random vector (Z'_U, W') and $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$,

$$J_{W, \lambda}(Z'_U | W') := \inf \{ I(W \wedge Z'_U | W') \mid (6.11a)$$

$$I_\lambda(Z'_U | W', W) = 0 \}. \quad (6.11b)$$

For any partition $\mathcal{P} \in \Pi'(U)$, $J_{W, \mathcal{P}}(Z'_U | W')$ (4.7) is the special case when λ satisfies (6.4). In the bivariate case $U = \{i, j\}$ where $i \neq j$, it reduces to $J_W(Z'_i \wedge Z'_j | W')$ [32]. □

A bound on the support size of W similar to Wyner common information can be imposed to make the computation more tractable.

Proposition 6.3 It is admissible to have $|W| \leq |Z'_U| |W'|$ in (6.11), in which the “inf” can be replaced by “min”. □

PROOF This follows from Lemma D.4 and (D.15) in Appendix D-3. ■

The desired lower bound on R_S is:

Theorem 6.1 For the general scenario $S \subsetneq A$, if we have

$$C_S = I_\lambda(Z_U | Z_D) \quad \text{for some } \lambda \in \Lambda(U, \mathcal{H}) \quad \text{where} \quad (6.12a)$$

$$U \subseteq V \text{ is such that } V \setminus D \setminus S \subseteq U \subseteq V \setminus D \quad \text{and} \quad (6.12b)$$

$$\mathcal{H} := \{B \subseteq U \mid \emptyset \neq B \not\subseteq A \cap U\}, \quad (6.12c)$$

then the communication complexity is lower bounded as

$$\begin{aligned} R_S &\geq \liminf_{n \rightarrow \infty} \frac{1}{n} H(F | \tilde{Z}_D) \\ &\geq J_{W, \lambda}(Z_U | Z_D) - I_\lambda(Z_U | Z_D), \end{aligned} \quad (6.13)$$

which is in fact a lower bound on the total discussion rate of the trusted users, since $H(F | \tilde{Z}_D) = H(F_{V \setminus D \setminus S} | \tilde{Z}_D)$. □

PROOF See Appendix D-3. ■

C. With helpers

In this section, we specialize the results to the scenario $A \subseteq V$ but $S = D = \emptyset$. This will be assumed throughout the section, unless otherwise stated.

Theorem 6.2 Let $\Lambda^*(A, Z_V)$ be the set of optimal fractional partitions in the characterization (6.6) of C_S by I_λ , and

$$\mathcal{H} := \{B, V \setminus B \mid B \in \text{supp}(\lambda^*), \lambda^* \in \Lambda^*(A, Z_V)\}. \quad (6.14)$$

Then,

$$R_S \geq \max_{\lambda^* \in \Lambda^*(A, Z_V)} J_{W, \lambda^*}(Z_V) - C_S \quad (6.15a)$$

$$\geq I_\lambda(Z_V) - C_S, \quad (6.15b)$$

for any $\lambda \in \Lambda(V, \mathcal{H})$. □

PROOF See Appendix D-4. ■

Theorem 6.3 $R_S = R_{CO}$ if, for \mathcal{H} defined in (6.14),

$$\exists \lambda \in \Lambda(V, \mathcal{H}), I_\lambda(Z_V) = H(Z_V), \quad (6.16)$$

i.e., $H(Z_B | Z_{V \setminus B}) = 0$ for all $B \in \text{supp}(\lambda)$. □

PROOF This follows immediately from Theorem 6.2 by making use of Proposition 6.1 with $D = S = \emptyset$. ■

Note that (4.11a) is the special case of (6.15a) when λ is chosen to be (6.4) for the fundamental partition $\mathcal{P}^*(Z_V)$, and (4.11b) is the special case of (6.15b) when λ is chosen to be (6.3) for the fundamental partition $\mathcal{P}^*(Z_V)$. The sufficient condition (4.12) in Theorem 4.2 also follows from Theorem 6.3 when λ satisfies (6.3) for the fundamental partition $\mathcal{P}^*(Z_V)$.

The following is an example taken from [9, Example A.1]. It has the property that the optimal λ^* to (6.6) is not the co-partition (i.e., the divergence upper bound [1, (26) in Example 4] is loose), unlike the case with no helpers in Theorem 4.1.

Example 6.1 Let Z_4, Z_5 and Z_6 be independent uniformly random bits, and define

$$Z_1 := Z_5 \oplus Z_6$$

$$Z_2 := Z_4 \oplus Z_6$$

$$Z_3 := Z_4 \oplus Z_5$$

With $V := [6]$ and $A = [3]$, it can be shown that

$$\Lambda^*(A, Z_V) = \{\lambda^*\} \text{ where}$$

$$\lambda^*(B) \in \left\{0, \frac{1}{4}\right\} \text{ for } B \subseteq V \setminus \{\emptyset\} \text{ and}$$

$$\text{supp}(\lambda^*) = \left\{ \{2, 3, 4\}, \{1, 3, 5\}, \{1, 2, 6\}, \right. \\ \left. V \setminus \{1\}, V \setminus \{2\}, V \setminus \{3\} \right\}.$$

Consider the fractional partition λ with

$$\lambda(B) := \begin{cases} \frac{1}{2} & \text{if } V \setminus B \in \text{supp}(\lambda^*) \\ 0 & \text{otherwise.} \end{cases}$$

It can be checked that $\lambda \in \Lambda(V, \mathcal{H})$ with \mathcal{H} defined in (6.14), using the fact that every $i \in V$ appears in exactly two subsets of $\text{supp}(\lambda)$, which is a subset of \mathcal{H} . We also have $I_\lambda(Z_V) = H(Z_V)$ since $H(Z_B | Z_{V \setminus B}) = 0$ for all $B \in$

$\text{supp}(\lambda)$. It follows from Theorem 6.3 that $R_S = R_{CO}$, and so omniscience is optimal. \square

The following example shows that not only is the lower bound (6.15) loose, but the sufficient condition is also not necessary, even for a simple PIN (Definition 3.3).

Example 6.2 Let X_a and X_b be uniformly random and independent bits. With $V := [3]$, let

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= (X_a, X_b) \\ Z_3 &:= X_b, \end{aligned}$$

which is the same as the source in Example 4.3 but with X_c removed. Consider $A = \{1, 3\}$, $S = D = \emptyset$. Then, C_S in (6.6) is 1, where the extremal⁶ optimal solutions are $\lambda^{(1)}$ and $\lambda^{(2)}$ defined as

$$\begin{aligned} \lambda^{(1)}(B) &= \begin{cases} 1 & \text{if } B \in \{\{1, 2\}, \{3\}\} \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \\ \lambda^{(2)}(B) &= \begin{cases} 1 & \text{if } B \in \{\{1\}, \{2, 3\}\} \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

It can be achieved non-asymptotically with $n = 1$ and $(K, F) = (X_a, X_a \oplus X_b)$. The support (6.14) for the optimal λ 's is $\mathcal{H} = \{\{1, 2\}, \{2, 3\}, \{1\}, \{3\}\}$. The lower bound on R_S given by Theorem 6.2 is trivial since $\lambda^{(1)}$ and $\lambda^{(2)}$ are the only feasible choices supported by \mathcal{H} , i.e., it is easy to see that $\Lambda(V, \mathcal{H}) = \{\lambda^{(1)}, \lambda^{(2)}\}$. However, by the result of [36], it can be shown that omniscience is indeed optimal in this case, i.e., $R_S = 1$. \square

D. With Silent Users

This section considers the scenario $S \subsetneq A = V$, i.e., all the users are active but some of them may be forced to be silent. This will be assumed throughout the section unless otherwise stated. We begin by providing an alternate characterization of the secrecy capacity in [2, Theorem 6].

Proposition 6.4

$$C_S = \begin{cases} \min_{i \in S} I(Z_{V \setminus S} \wedge Z_i) & \text{if } |V \setminus S| = 1 \\ \min\{\alpha, I(Z_{V \setminus S})\} & \text{if } |V \setminus S| > 1, \end{cases} \quad (6.18a)$$

$$(6.18b)$$

where $\alpha := \min_{i \in S} I(Z_{V \setminus S} \wedge Z_i)$. \square

PROOF See Appendix D-5 \blacksquare

The result can be easily extended to the case with untrusted helpers, i.e., $S \subsetneq A = V \setminus D$ with D possibly non-empty. To be precise, we have

$$C_S = \begin{cases} \min_{i \in S} I(Z_{(V \setminus D) \setminus S} \wedge Z_i | Z_D) & \text{if } |(V \setminus D) \setminus S| = 1 \\ \min\{\alpha, I(Z_{(V \setminus D) \setminus S} | Z_D)\} & \text{if } |(V \setminus D) \setminus S| > 1 \end{cases}$$

where $\alpha := \min_{i \in S} I(Z_{(V \setminus D) \setminus S} \wedge Z_i | Z_D)$.

⁶All other solutions can be expressed as convex combinations of the extremal solutions.

We now turn our attention to lower bounding R_S for the case with $S \subsetneq A = V$. For this, we introduce some convenient notation, starting with the definition

$$S^* := \{i \in S \mid I(Z_{V \setminus S} \wedge Z_i) = \alpha\}, \quad (6.19)$$

where α is as defined in Proposition 6.4. We extend the notation introduced in Theorem 4.1: for any $U \subseteq V$, the \mathcal{P}^* in the subscripts of $J_{W, \mathcal{P}^*}(Z_U)$, $J_{D, \mathcal{P}^*}(Z_U)$ and $I_{\mathcal{P}^*}(Z_U)$ denotes the fundamental partition $\mathcal{P}^*(Z_U)$.

Applying the lower bound in Theorem 4.1 with an appropriate choice of U and $\mathcal{P} \in \Pi'(U)$ yields the following result.

Theorem 6.4

$$R_S \geq \begin{cases} J_{W, \mathcal{P}^*}(Z_{V \setminus S}) - I(Z_{V \setminus S}) & \text{if } I(Z_{V \setminus S}) < \alpha \text{ and } |V \setminus S| > 1, \\ \max_{i \in S^*} J_{W, \mathcal{P}^*}(Z_{V \setminus S} \wedge Z_i) - \alpha, & \text{if } |V \setminus S| = 1, \\ \text{or, if } I(Z_{V \setminus S}) > \alpha \text{ and } |V \setminus S| > 1, \\ \max_{i \in S^*} J_{W, \mathcal{P}^*}(Z_{(V \setminus S) \cup \{i\}}) - \alpha, & \text{if } I(Z_{V \setminus S}) = \alpha \text{ and } |V \setminus S| > 1, \end{cases} \quad (6.20a)$$

$$(6.20b)$$

$$(6.20c)$$

where S^* is as defined in (6.19). \square

PROOF See Appendix D-5 \blacksquare

The lower bounds in Theorem 6.4 can be weakened by replacing $J_{W, \mathcal{P}}$ with the more easily computable $J_{D, \mathcal{P}}$. Using arguments similar to those in Section IV, we arrive at the following sufficient condition for $R_S = R_{CO}$ to hold.

Theorem 6.5

- $R_S = R_{CO}$ in either of the following scenarios:
- (i) $H(Z_C | Z_{V \setminus C}) = 0, \forall C \in \mathcal{P}^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < \alpha$,
 - (ii) $\exists i \in S^*$ such that $H(Z_{V \setminus S} | Z_i) = 0$, when $|V \setminus S| = 1$, or when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$,
 - (iii) $\exists i \in S^*$ such that $H(Z_C | Z_{V \setminus S \setminus C}, Z_i) = 0, \forall C \in \mathcal{P}^*(Z_{V \setminus S}) \cup \{i\}$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = \alpha$,

where S^* is as defined in (6.19). \square

PROOF See Appendix D-5 \blacksquare

Example 6.3 Consider the PIN in Example 6.2 with $A = V = [3]$. We consider the following cases:

- $S = \{3\}$: It is easy to verify that $I(Z_{V \setminus S}) = 1$ with $\mathcal{P}^*(Z_{V \setminus S}) = \{\{1\}, \{2\}\}$, and $\alpha = I(Z_{\{1, 2\}} \wedge Z_3) = 1 = I(Z_{V \setminus S})$. It is obvious that $S^* = S = \{3\}$. Therefore, the condition for Theorem 6.5.(iii) holds and so $R_S = R_{CO}$.
- $S = \{2\}$: Again, it is easy to verify that $I(Z_{V \setminus S}) = I(Z_{\{1, 3\}}) = 0$ and $\mathcal{P}^*(Z_{V \setminus S}) = \{\{1\}, \{3\}\}$. Also, $\alpha = I(Z_{\{1, 3\}} \wedge Z_2) = 2 > I(Z_{V \setminus S})$. Now, as $H(Z_3 | Z_1) = 1 > 0$, Theorem 6.5.(i) fails to confirm whether $R_S = R_{CO}$. However, it is easy to see that $C_S = 0$ and $R_{CO} = 2$, which follows using Theorem 6 of [2] and Proposition 6.4. Therefore, $R_S = 0$ holds trivially, and hence $R_S < R_{CO}$.

- $S = \{1, 3\}$: In this case, we have $|V \setminus S| = 1$ and see that $\alpha = \min\{I(Z_2 \wedge Z_3), I(Z_2 \wedge Z_1)\} = 1$, with $S^* = S = \{1, 3\}$. However, it turns out that $H(Z_2|Z_i) = 1 > 0$, $i = 1, 3$, and hence Theorem 6.5(ii) is unable to conclude whether $R_S = R_{CO}$.

We remark here that for the special case of a hypergraphical source (as defined in Definition 3.2), the sufficient conditions in Theorem 6.5 can be strengthened to a necessary and sufficient condition for $R_S = R_{CO}$. (See Theorem 6.7.) Using the stronger result, we can show that $R_S = R_{CO}$ holds for the last case when $S = \{1, 3\}$. \square

E. The Hypergraphical Source with Silent Users

In this section, we restrict our attention to the hypergraphical source with silent users, i.e., $S \subsetneq A = V$. The goal of this section is to strengthen the sufficient conditions for $R_S = R_{CO}$ given in Theorem 6.5. We will show that the strengthened conditions are both necessary and sufficient for $R_S = R_{CO}$ to be valid, as promised in Example 6.3.

The idea is based on the following observation.

Proposition 6.5 *For any hypergraphical source, (V, E, ξ) , C_S, R_S and R_{CO} remain unchanged by removing any hyper-edge $e' \in E$ such that $\xi(e') \subseteq S$.* \square

PROOF See Appendix D-6 \blacksquare

Thanks to this fact we will assume that the hypergraphical sources considered later in this section satisfy

$$\forall e \in E, \xi(e) \not\subseteq S. \quad (6.21)$$

Using (6.21), the lower bound in Theorem 6.4 can be strengthened to the following for the hypergraphical source.

Theorem 6.6 *For any hypergraphical source (V, E, ξ) with $S \subsetneq A = V$, we have*

$$R_S \geq \begin{cases} J_{W, \mathcal{P}^*}(Z_{V \setminus S}) - I(Z_{V \setminus S}) & \text{if } I(Z_{V \setminus S}) < \alpha \text{ and } |V \setminus S| > 1, \\ J_{W, (V \setminus S) \cup \{i\} | i \in S^*}(Z_{(V \setminus S) \cup S^*}) - \alpha, & \text{if } |V \setminus S| = 1, \\ \text{or, if } I(Z_{V \setminus S}) > \alpha \text{ and } |V \setminus S| > 1, & (6.22b) \\ J_{W, \mathcal{P}^*}(Z_{V \setminus S}) - I(Z_{V \setminus S}) & \text{if } I(Z_{V \setminus S}) = 1 \text{ and } |V \setminus S| > 1, \end{cases} \quad (6.22a)$$

where S^* is as defined in (6.19). \square

PROOF See Appendix D-6 \blacksquare

The results of Theorem 6.6 can be used to obtain sufficient conditions for $R_S = R_{CO}$ to hold, by following the same steps as in the proof of Theorem 6.5. Fortunately, it turns out that those conditions are also necessary, a fact that can be proved using the idea of decremental secret key agreement highlighted in [37].

Theorem 6.7 *For any hypergraphical source (V, E, ξ) with $S \subsetneq A = V$, we have $R_{CO} = R_S$ iff*

- (i) $H(Z_C|Z_{V \setminus C}) = 0, \forall C \in \mathcal{P}^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < \alpha$,
- (ii) $H(Z_{V \setminus S}|Z_{S^*}) = 0$, when $|V \setminus S| = 1$ or, if $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$,
- (iii) $H(Z_C|Z_{((V \setminus S) \cup S^*) \setminus C}) = 0, \forall C \in \mathcal{P}^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = \alpha$. \square

PROOF See Appendix D-6 \blacksquare

F. With Untrusted Users

The lower bounds and sufficient conditions derived so far (Theorems 4.2–4.3 and Theorems 6.2–6.7) can all be extended to the case with untrusted helpers by further conditioning on Z_D in the entropies, as in Theorem 6.1. For hypergraphical sources, this is equivalent to removing the hyperedges incident on D , as in Corollary 5.5.

VII. CHALLENGES

In this section, we conclude our work by explaining some challenges that remain and techniques that potentially improve the results derived so far.

A. Limitation

We first show that the sufficient condition in Theorem 4.2 for the optimality of omniscience may not be necessary for the following example from [17], resolving the conjecture therein.

Example 7.1 Let X_a, X_b, X_c and X_d be uniformly random and independent bits, and define

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= X_b \\ Z_3 &:= X_c \\ Z_4 &:= (X_a, X_b, X_c \oplus X_d) \\ Z_5 &:= (X_a, X_b, X_d). \end{aligned}$$

With $A = V := [5]$ and $S = \emptyset$, it can be shown that

$$\begin{aligned} C_S &= I(Z_V) = 1 \text{ with } \mathcal{P}^*(Z_V) = \{\{1\}, \{2\}, \{3\}, \{4, 5\}\} \\ R_{CO} &= H(Z_V) - C_S = 3 \\ J_{W, \mathcal{P}^*}(Z_V) &= J_{D, \mathcal{P}^*}(Z_V) = 3 < H(Z_V) = 4 \end{aligned}$$

with $W = (X_{\{a, b, c\}})$. To achieve the capacity, we can choose for $n = 1$

$$\begin{aligned} K &:= Z_1 = X_a \\ F_4 &:= X_c \oplus X_d \\ F_5 &:= (X_a \oplus X_b, X_a \oplus X_d), \end{aligned}$$

which also achieves omniscience at the minimum rate.

Note that the sufficient condition (4.12) for the optimality of omniscience does not hold because

$$H(Z_{\{4, 5\}}|Z_{\{1, 2, 3\}}) = H(X_d, X_c \oplus X_d|X_c) = 1 > 0.$$

The following result will show that omniscience is indeed optimal for this example, and so the sufficient condition is not necessary. Furthermore, since the sufficient condition is derived from the lower bound (4.11) on R_S , the bound is also loose for this example. \square

Proposition 7.1 For Example 7.1, $R_S = R_{CO}$. \square

PROOF See Appendix E-1. \blacksquare

B. Potential Improvements

In this section, we give some potential improvements of the lower bound by a change of scenario.

Theorem 7.1 C_S and R_S remain unchanged by the following change of user sets:

- (i) A vocal untrusted user is turned into a silent untrusted user, and a new trusted helper with the same private source as the original vocal untrusted user is added. That is to say, (S, V) becomes $(S \cup \{i\}, V \cup \{i'\})$ for some $i \in D \setminus S$ and with $i' \notin V$ being a new user with private source $Z_{i'} = Z_i$ identical to that of i .
- (ii) A trusted helper $i \in V \setminus A \setminus S \setminus D$ with $H(Z_i|Z_j) = 0$ for some vocal user $j \in V \setminus S$ is removed, i.e., V becomes $V \setminus \{i\}$. \square

PROOF See Appendix E-2 \blacksquare

Theorem 7.2 Suppose (C_S, R_S) becomes (C'_S, R'_S) by one of the following change of user sets:

- (i) a silent user is removed, i.e., (A, S, D, V) becomes $(A, S \setminus \{i\}, D \setminus \{i\}, V \setminus \{i\})$ for some $i \in S \cap D$, or $(A \setminus \{i\}, S \setminus \{i\}, D, V \setminus \{i\})$ for some $i \in A \cap S$.
- (ii) a silent active user is turned into a vocal active user, i.e., S becomes $S \setminus \{i\}$ for some $i \in A \cap S$.

Then, $C'_S \geq C_S$. If equality holds, then $R'_S \leq R_S$. \square

PROOF See Appendix E-2 \blacksquare

Example 7.2 Let X_a and X_b be independent uniformly random bits. Consider the PIN in Example 6.2 but with user 4 added so that the private source consists of

$$\begin{aligned} Z_1 &:= X_a \\ Z_2 &:= (X_a, X_b) \\ Z_3 &:= X_b \\ Z_4 &:= X_b \end{aligned}$$

Suppose $(A, S, D) = ([3], \{1, 3\}, \emptyset)$. It can be shown that $C_S = R_{CO} = 1$, which is achievable non-asymptotically with $n = 1$ and $(K, F) = (Z_1, F_2) = (Z_a, Z_a \oplus Z_b)$. We can apply (ii) in Theorem 7.1 to remove the trusted user 4, since $H(Z_4|Z_2) = 0$ and $2 \in V \setminus S$. With V changed to $V' = \{1, 2, 3\}$, the C_S and R_S remain unchanged. Since the model is hypergraphical (in particular, a PIN), we can apply Theorem 6.6 to show that R_S of the new scenario is at least 1, and so $R_S = R_{CO} = 1$ in the original scenario by Theorem 7.1 \square

The following conjectures, if proven correct, can further improve the lower bound (6.13). They are true if one can prove the stronger conjecture in [16] that private randomization does not decrease R_S .

Conjecture 1 R_S does not increase by

- (i) making a trusted helper active provided that the private source of the helper determines that of another active user.
- (ii) forcing a vocal active user silent if its source is determined by that of another vocal user. \square

Example 7.3 Consider the PIN in Example 6.2 with $V = [3]$. Let $(A, S, D) = (\{1, 3\}, \emptyset, \emptyset)$. As discussed in Example 6.2, the lower bound (6.13) fails to show $R_S \geq 1$. However, if the conjecture above is proved, then we could apply (i) in the conjecture to turn the trusted helper into an active vocal user, in which case $R_S = 1$ as described in the previous example for the new scenario. \square

APPENDIX A

PROOF OF PROPOSITION 3.1

Consider $j \in D$ first. As will be useful to a later result, we will prove the stronger statement that U_j neither increases C_S nor decreases R_S even when U_j is a public randomization [12] observed by everyone in addition to the wiretapper, i.e., with (3.5) modified to have F_i depend directly on U_j . To do so, it suffices to show that the recoverability (3.7) and secrecy (3.8) constraints continue to hold even if U_j is chosen to be deterministic. More precisely, for any $\delta > 0$, let

$$U_j(\delta) := \left\{ u \in U_j \mid \Pr(\exists i \in A, K \neq \theta_i(\tilde{Z}_i, F) \mid U_j = u) \leq \delta, \right. \quad (\text{A.1a})$$

$$\left. \frac{1}{n} [\log |K| - H(K|F, \tilde{Z}_D, U_j = u)] \leq \delta \right\}. \quad (\text{A.1b})$$

We have the desired result if $U_j(\delta_n) \neq \emptyset$ for some $\delta_n \rightarrow 0$ since, by choosing U_j to be deterministically equal to any element in $U_j(\delta_n)$, (A.1a) and (A.1b) implies (3.7) and (3.8) respectively. Indeed, not only can we show that $U_j(\delta) \neq \emptyset$, i.e., $\Pr(U_j \in U_j(\delta)) > 0$, but also that

$$\lim_{n \rightarrow \infty} \Pr(U_j \in U_j(\delta)) = 1 \quad \forall \delta > 0. \quad (\text{A.2})$$

Let $U'_j(\delta)$ be the set $U_j(\delta)$ in (A.1) with only (A.1a) (but not (A.1b)) imposed. Similarly, let $U''_j(\delta)$ to be the set with only (A.1b) imposed. It follows that

$$U_j(\delta) = U'_j(\delta) \cap U''_j(\delta)$$

and so, by the union bound,

$$\Pr(U_j \in U_j(\delta)) \geq 1 - \Pr(U_j \notin U'_j(\delta)) - \Pr(U_j \notin U''_j(\delta)).$$

It suffices to show that the last two probabilities go to 0 asymptotically in n . By the Markov inequality,

$$\begin{aligned} \Pr(U_j \notin U'_j(\delta)) &\leq \frac{\Pr(\exists i \in A, K \neq \theta_i(\tilde{Z}_i, F))}{\delta} \\ \Pr(U_j \notin U''_j(\delta)) &\leq \frac{\frac{1}{n} [\log |K| - H(K|F, \tilde{Z}_D, U_j)]}{\delta}. \end{aligned}$$

The bounds go to zero as desired by (3.7) and (3.8), hence completing the proof of (A.2).

Consider the remaining case $j \in S$. (Unlike the previous case, we do not consider U_j is a public randomization here.) Note that

$$I(U_j \wedge \tilde{Z}_{V \setminus \{j\}}, F) = 0 \quad (\text{A.3})$$

because F in (3.5) does not depend on U_j as user j is silent, and the U_j is independent of $\tilde{Z}_{V \setminus \{j\}}$ by the assumption (3.11). We will show that this implies that

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(U_j \wedge K|F, \tilde{Z}_D) = 0 \quad (\text{A.4})$$

Since $|A| \geq 2$, there exists another active user, say $i \in A \setminus \{j\}$. By the recoverability condition (3.7) for user i (which does not depend on U_j), we have

$$\lim_{n \rightarrow \infty} \Pr\{K \neq \theta_i(\tilde{Z}_i, F)\} = 0$$

which gives

$$I(U_j \wedge K|F, \tilde{Z}_D) \stackrel{(a)}{\leq} I(U_j \wedge \tilde{Z}_i, F|F, \tilde{Z}_D) + n\delta_n \stackrel{(b)}{=} n\delta_n$$

for some $\delta_n \rightarrow 0$. Here, (a) follows from Fano's inequality, and (b) is because

$$\begin{aligned} I(U_j \wedge \tilde{Z}_i, F|F, \tilde{Z}_D) &\leq I(U_j \wedge \tilde{Z}_i, F, \tilde{Z}_D) \\ &\leq I(U_j \wedge \tilde{Z}_{V \setminus \{j\}}, F), \end{aligned}$$

which equals zero by (A.3), completing the proof of (A.4).

Now, by (3.8),

$$\begin{aligned} 0 &= \lim_{n \rightarrow \infty} \frac{1}{n} [\log|K| - H(K|F, \tilde{Z}_D)] \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} [\log|K| - H(K|F, \tilde{Z}_D, U_j)] \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} [\log|K| - \max_{u \in U_j} H(K|F, \tilde{Z}_D, U_j = u)] \end{aligned}$$

where the second equality follows from (A.4). Hence, by setting $U_j = u$ deterministically, (3.8) remains to hold (since $\max_{u \in U_j} H(K|F, \tilde{Z}_D, U_j = u) = H(K|F, \tilde{Z}_D)$ in the above). Furthermore, (3.7) (without U_j) also hold by (A.4). This completes the proof of the proposition.

APPENDIX B PROOFS FOR SECTION IV

1. Proof of Theorem 4.1

It is enough to prove (4.11a), since (4.11b) then follows from (4.9). Let U_V be the optimal sequence of randomization that achieves R_S , and let $R_S^{\text{NR}}(\tilde{Z}_V)$ be the communication complexity when the source Z_V is changed to \tilde{Z}_V instead (see (3.4) for the definition of \tilde{Z}_V). Then,

$$\begin{aligned} R_S(Z_V) &\stackrel{(a)}{\geq} \frac{1}{n} R_S^{\text{NR}}(\tilde{Z}_V) \stackrel{(b)}{\geq} \frac{1}{n} [C_W(\tilde{Z}_V) - I(\tilde{Z}_V)] \\ &\stackrel{(c)}{\geq} \frac{1}{n} [nJ_{W, \mathcal{P}^*}(Z_V) - I(\tilde{Z}_V)] \\ &\stackrel{(d)}{=} J_{W, \mathcal{P}^*}(Z_V) - I(Z_V) \end{aligned}$$

- To explain (a), note that the secrecy capacity of the new scenario is nC_S , since randomization does not change the secrecy capacity [1]. Any optimal scheme that achieves

R_S for the original scenario can therefore be translated directly to a scheme that achieves nR_S for the new scenario without randomization.

- (b) is by Proposition 4.5 with Z_V replaced by \tilde{Z}_V , and $C_W(\tilde{Z}_V)$ denoting the corresponding multi-letter multi-variate Wyner common information (4.5).
- (c) follows from

$$C_W(\tilde{Z}_V) \geq nJ_{W, \mathcal{P}^*}(Z_V), \quad (\text{B.1})$$

which will be argued in more detail later.

- To explain (d), note that for all $B \subseteq V$,

$$\begin{aligned} H(\tilde{Z}_B) &= H(Z_B^n, U_B) \\ &= nH(Z_B) + H(U_B), \end{aligned}$$

which gives

$$I_{\mathcal{P}}(\tilde{Z}_V) = nI_{\mathcal{P}}(Z_V) + I_{\mathcal{P}}(U_V)$$

for all $\mathcal{P} \in \Pi'(V)$. Since $I_{\mathcal{P}}(U_V) = 0$ by the fact that the U_i 's are mutually independent (3.3), the above equation implies $I(\tilde{Z}_V) = nI(Z_V)$ as desired.

To explain (B.1), consider the optimal sequence in n' of L to $C_W(\tilde{Z}_V)$. By standard arguments,

$$\begin{aligned} H(L) &\geq I(\tilde{Z}_V^{n'} \wedge L) \geq I(Z_V^{nn'} \wedge L) \\ &= H(Z_V^{nn'}) - H(Z_V^{nn'} | L) \\ &= \sum_{t=1}^{nn'} H(Z_{Vt}) - \sum_{t=1}^{nn'} H(Z_{Vt} | Z_V^{t-1}, L) \end{aligned}$$

where the second inequality follows from the usual data processing inequality (see (6.10a)) since Z_V^n is determined by \tilde{Z}_V , and so, we have the Markov chain $L - \tilde{Z}_V^{n'} - Z_V^{nn'}$. Let J be the usual time-sharing random variable uniformly distributed over $[nn']$ and independent of everything else, namely $(\tilde{Z}_V^{n'}, L)$, and define

$$W_J := (J, Z_V^{J-1}, L).$$

Then, the above inequality gives

$$\frac{1}{n'} H(L) \geq nI(Z_V \wedge W_J). \quad (\text{B.2})$$

On the other hand, we can also bound $I_{\mathcal{P}^*}$ in the constraint (4.5b) of C_W as follows:

$$\begin{aligned} I_{\mathcal{P}^*}(\tilde{Z}_V)(\tilde{Z}_V^{n'} | L) &\geq I_{\mathcal{P}^*}(Z_V)(Z_V^{nn'} | L) \\ &= \frac{1}{|\mathcal{P}^*| - 1} \left[\sum_{C \in \mathcal{P}^*} \underbrace{H(Z_C^{nn'} | L)}_{\textcircled{1}} - \underbrace{H(Z_V^{nn'} | L)}_{\textcircled{2}} \right] \end{aligned}$$

where, as in the statement of the theorem, \mathcal{P}^* denotes $\mathcal{P}^*(Z_V)$ for convenience. In the above inequality, we have applied $\mathcal{P}^*(\tilde{Z}_V) = \mathcal{P}^*(Z_V)$ and the data processing inequality [9, (5.20b)] since Z_i^n is determined by \tilde{Z}_i . (See also (6.8) with I_λ

reduced to $I_{\mathcal{P}}$ by restricting λ to (6.4.) Expanding ① and ② by the chain rule,

$$\begin{aligned} \textcircled{1} &= \sum_{t=1}^{nn'} H(Z_{Ct} | \mathbf{L}, Z_C^{t-1}) \\ &\geq \sum_{t=1}^{nn'} H(Z_{Ct} | \mathbf{L}, Z_V^{t-1}) = nn' H(Z_{CJ} | \mathbf{W}_J) \\ \textcircled{2} &= \sum_{t=1}^{nn'} H(Z_{Vt} | \mathbf{L}, Z_V^{t-1}) = nn' H(Z_{VJ} | \mathbf{W}_J). \end{aligned}$$

Altogether, we have

$$\begin{aligned} \frac{1}{n'} I_{\mathcal{P}^*}(\tilde{Z}_V)(\tilde{Z}_V^{n'} | \mathbf{L}) \\ \geq \frac{n}{|\mathcal{P}^*| - 1} \left[\sum_{C \in \mathcal{P}^*} H(Z_{CJ} | \mathbf{W}_J) - H(Z_{VJ} | \mathbf{W}_J) \right] \\ = n I_{\mathcal{P}^*}(Z_{VJ} | \mathbf{W}_J), \end{aligned} \quad (\text{B.3})$$

Now, for $\delta \geq 0$, define

$$\Gamma(\delta) := \sup_{P_{W|Z_V} : I_{\mathcal{P}^*}(Z_V | W) \leq \delta} H(Z_V | W), \quad (\text{B.4})$$

where the supremum is over all possible choices of the conditional distribution $P_{W|Z_V}$. The expression depends implicitly on the distribution P_{Z_V} . It follows that

$$\Gamma\left(\frac{1}{nn'} I_{\mathcal{P}^*}(\tilde{Z}_V)(\tilde{Z}_V^{n'} | \mathbf{L})\right) \geq H(Z_{VJ} | \mathbf{W}_J)$$

since Z_{VJ} has the same distribution as Z_V and so the conditional distribution $P_{W_J|Z_{VJ}}$ is a feasible solution to (B.4) with δ chosen appropriately from the bound (B.3) on $I_{\mathcal{P}^*}(Z_{VJ} | \mathbf{W}_J)$. Together with (B.2), we have

$$\begin{aligned} C_W(\tilde{Z}_V) &\geq \lim_{n' \rightarrow \infty} n \left[H(Z_{VJ}) - \Gamma\left(\frac{1}{nn'} I_{\mathcal{P}^*}(\tilde{Z}_V)(\tilde{Z}_V^{n'} | \mathbf{L})\right) \right] \\ &= n \left[H(Z_V) - \lim_{\delta \rightarrow 0} \Gamma(\delta) \right] \end{aligned}$$

where the last equality is because $H(Z_{VJ}) = H(Z_V)$ and $\frac{1}{n'} I_{\mathcal{P}^*}(\tilde{Z}_V)(\tilde{Z}_V^{n'} | \mathbf{L})$ goes to 0 as n' goes to ∞ by the constraint (4.5b) for $C_W(\tilde{Z}_V)$. It can be shown that $\Gamma(\delta)$ is continuous in δ using the same argument as in [32]. For completeness, this is proved for the more general case in Lemma D.4 in Appendix D-3. Hence,

$$\begin{aligned} C_W(\tilde{Z}_V) &\geq n [H(Z_V) - \Gamma(0)] \\ &= n J_{W, \mathcal{P}^*}(Z_V) \end{aligned}$$

by the definition (4.7) of $J_{W, \mathcal{P}}$.

2. Proof of Theorem 4.3

To prove Theorem 4.3, we use the idea of decremental secret key agreement [37, Theorem 4.2].

Proposition B.1 ([37, Theorem 4.2]) *If Z_V can be rewritten for some $T \subseteq C \in \mathcal{P}^*(Z_V)$ as*

$$Z_i = \begin{cases} (\hat{Z}_i, \mathbf{X}) & \forall i \in T \\ \hat{Z}_i & \forall i \in V \setminus T, \end{cases} \quad (\text{B.5})$$

where $H(\mathbf{X}) = H(\mathbf{X} | \hat{Z}_V) > 0$, then, we have

$$H(Z'_V) < H(Z_V) \quad \text{and} \quad I(Z'_V) = I(Z_V) \quad (\text{B.6})$$

for some function $Z'_i = \vartheta_i(Z_i)$ for $i \in V$. \square

Roughly speaking, when (4.12) fails for hypergraphical sources, we can identify and reduce excess randomness in the source without changing C_S , and so omniscience is not optimal in achieving R_S .

The “if” case of Theorem 4.3 follows from Theorem 4.2 directly. To prove the “only if” part, suppose to the contrary that

$$H(Z_C | Z_{V \setminus C}) > 0 \quad \text{for some } C \in \mathcal{P}^*(Z_V).$$

For hypergraphical model, this means that

$$H(\mathbf{X}_{e'} | Z_{V \setminus C}) > 0 \quad \text{for some } e' \in E,$$

i.e., $\xi(e') \subseteq C$. Thus, (B.5) holds with $\mathbf{X} := \mathbf{X}_{e'}$, $T := \xi(e') \subseteq C$ and

$$\hat{Z}_i := (\mathbf{X}_e \mid e \in E \setminus e', i \in \xi(e)).$$

By Proposition B.1, we have (B.6). With R'_S and R'_{CO} denoting the communication complexity and the smallest rate of CO for the source Z'_V , we have

$$\begin{aligned} R_S &\stackrel{(a)}{\leq} R'_S \leq R'_{CO} = H(Z'_V) - I(Z'_V) \\ &\stackrel{(b)}{<} H(Z_V) - I(Z_V) = R_{CO}(Z_V), \end{aligned}$$

where (a) is due to the fact that processing Z_i 's individually cannot reduce the communication complexity R_S ; and (b) is by (B.6). This completes the proof of Theorem 4.3.

3. Proof of Proposition 4.8

First, observe that with $W = (\mathbf{X}_e \mid e \in E^*)$, using the assumption that the random variables \mathbf{X}_e 's are mutually independent, we have

$$\begin{aligned} \sum_{C \in \mathcal{P}^*} H(Z_C | W) &= \sum_{C \in \mathcal{P}^*} H(\mathbf{X}_{\{e \in E \setminus E^* \mid \xi(e) \subseteq C\}}) \\ &= H(\mathbf{X}_{\{E \setminus E^*\}}) = H(Z_V | W) \end{aligned}$$

Hence, $I_{\mathcal{P}^*}(Z_V | W) = 0$, and so W is a feasible solution to $J_{W, \mathcal{P}^*}(Z_V)$. Thus, $J_{W, \mathcal{P}^*}(Z_V) \leq H(\mathbf{X}_{E^*})$. By (4.9), On the other hand, we also have, by (4.9),

$$\begin{aligned} J_{W, \mathcal{P}^*}(Z_V) &\geq H(Z_V) - \sum_{C \in \mathcal{P}^*} H(Z_C | Z_{V \setminus C}) \\ &= H(\mathbf{X}_E) - \sum_{C \in \mathcal{P}^*} H(\mathbf{X}_{\{e \in E \setminus E^* \mid \xi(e) \subseteq C\}}) \\ &= H(\mathbf{X}_E) - H(\mathbf{X}_{\{E \setminus E^*\}}) \\ &= H(\mathbf{X}_{E^*}) \end{aligned}$$

Thus, $J_{W, \mathcal{P}^*}(Z_V) = H(\mathbf{X}_{E^*})$ with $W = (\mathbf{X}_e \mid e \in E^*)$ being an optimal solution.

APPENDIX C
PROOFS FOR SECTION V

1. Proof of Theorem 5.1

Converse proof of C_S :

We first prove ‘ \leq ’ for (5.1) by making use of the following result that directly extends the technique of the converse proof of [1, Theorem 2] and [2, Theorem 6].

Lemma C.1 For any $B \subseteq V \setminus D \setminus S$, we have

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(K|F, \tilde{Z}_{V \setminus S \setminus B}) \geq H(Z_B|Z_{V \setminus S \setminus B}) - r(B) \quad (\text{C.1a})$$

$$\text{with } r_i := \limsup_{n \rightarrow \infty} \frac{1}{n} \left[\sum_{t \in [r]} H(F_{it} | \tilde{F}_{it}, \tilde{Z}_D) + H(\tilde{Z}_i | \tilde{Z}_D, \tilde{Z}_{[i-1]}, K, F) - H(U_i) \right]. \quad (\text{C.1b})$$

The inequality is satisfied with equality if $B = V \setminus D \setminus S$. \square

This completes the proof because, by the secrecy constraint (3.8),

$$\begin{aligned} \liminf_{n \rightarrow \infty} \frac{1}{n} \log |K| &\leq \limsup_{n \rightarrow \infty} \frac{1}{n} H(K|F, \tilde{Z}_D) \\ &= H(Z_{V \setminus D \setminus S} | Z_D) - r(V \setminus D \setminus S) \end{aligned}$$

by the equality case of (C.1a) with $B = V \setminus D \setminus S$. Moreover, $r_{V \setminus D \setminus S}$ satisfies (5.3b) because, for any $j \in A$ and $B \subseteq V \setminus D \setminus S \setminus \{j\}$, the limit in (C.1a) is 0 by Fano’s inequality and the recoverability constraint (3.7) as $j \in V \setminus S \setminus B$. (Note that the constraints for $B \ni j$ are redundant.)

PROOF (LEMMA C.1) By the assumption (3.3) of the private randomizations and the memorylessness of the private source,

$$H(\tilde{Z}_B | \tilde{Z}_{V \setminus S \setminus B}) = \sum_{i \in B} H(U_i) + nH(Z_B | Z_{V \setminus S \setminus B}).$$

Alternatively, since F is determined by $\tilde{Z}_{V \setminus S}$ by (3.5), we have

$$\begin{aligned} H(\tilde{Z}_B | \tilde{Z}_{V \setminus S \setminus B}) &= H(F, \tilde{Z}_B | \tilde{Z}_{V \setminus S \setminus B}) \\ &= \underbrace{H(K, F, \tilde{Z}_B | \tilde{Z}_{V \setminus S \setminus B})}_{\textcircled{1}} - n\delta_n \end{aligned}$$

where $\delta_n := \frac{1}{n} H(K|F, \tilde{Z}_{V \setminus S})$ goes to 0 as $n \rightarrow \infty$ by Fano’s inequality because K can be recovered from $(F, \tilde{Z}_{V \setminus S})$ asymptotically by (3.7), due to the assumption $S \subsetneq A$ that there must be at least one vocal active user, i.e., $A \cap (V \setminus S) \neq \emptyset$. Expanding the last entropy term $\textcircled{1}$ by the chain rule gives

$$\begin{aligned} \textcircled{1} &= \overbrace{H(F | \tilde{Z}_{V \setminus S \setminus B})}^{\textcircled{2}} + \overbrace{H(K | F, \tilde{Z}_{V \setminus S \setminus B})}^{\textcircled{3}} + \overbrace{H(\tilde{Z}_B | K, F, \tilde{Z}_{V \setminus S \setminus B})}^{\textcircled{3}} \\ &= \sum_{t \in [r]} \sum_{i \in V \setminus S} H(F_{it} | \tilde{F}_{it}, \tilde{Z}_{V \setminus S \setminus B}) \\ &\stackrel{(a)}{=} \sum_{i \in B} \sum_{t \in [r]} H(F_{it} | \tilde{F}_{it}, \tilde{Z}_{V \setminus S \setminus B}) \stackrel{(b)}{\leq} \sum_{i \in B} \sum_{t \in [r]} H(F_{it} | \tilde{F}_{it}, \tilde{Z}_D) \\ \textcircled{3} &= \sum_{i \in B} H(\tilde{Z}_i | \tilde{Z}_{(V \setminus S \setminus B) \cup [i-1]}, K, F) \\ &\stackrel{(c)}{\leq} \sum_{i \in B} H(\tilde{Z}_i | \tilde{Z}_D, \tilde{Z}_{[i-1]}, K, F), \end{aligned}$$

where (a) is because the entropy terms for $i \notin B$ are zero by (3.5). Rearranging the terms give (C.1) with the desired equality condition because inequalities (b) and (c) holds with equality if $B = V \setminus D \setminus S$. \blacksquare

Characterization of R_{CO} :

Next, we prove the characterization of R_{CO} in (5.2). For each $j \in A$, let

$$\mathcal{R}'(Z_{V \setminus D \setminus S} | Z_{D \cup \{j\}}) := \{r_{V \setminus D \setminus S} \in \mathbb{R}^{V \setminus D \setminus S} \mid \quad (\text{C.2a})$$

$$r(B) \geq H(Z_B | Z_{V \setminus S \setminus B}, Z_j) \forall B \subseteq V \setminus D \setminus S\} \quad (\text{C.2b})$$

$$\mathcal{R}'(Z_D | Z_j) := \{r_D \in \mathbb{R}^D \mid \quad (\text{C.2c})$$

$$r(B) \geq H(Z_B | Z_{D \setminus B}, Z_j) \forall B \subseteq D\} \quad (\text{C.2d})$$

Note that, by the standard result of independent source coding with side information, $\mathcal{R}'_j(Z_{V \setminus D \setminus S} | Z_{D \cup \{j\}})$ is the set of achievable rate tuple for encoding each components of the source $Z_{V \setminus D \setminus S}$ independently so that they can be recovered from the codewords given the source $Z_{D \cup \{j\}}$ as side information. The omniscience constraint (3.13b) requires the recoverability simultaneously for all $j \in A$, and so the achievable rate region is

$$\bigcap_{j \in A} \mathcal{R}'_j(Z_{V \setminus D \setminus S} | Z_{D \cup \{j\}})$$

by the result of normal source network [4, Chapter 1]. ρ in (5.3a) is the minimum sum rate over this region because (5.3b) is composed of (C.2b) for all $j \in A$. Similarly, it can be argued that

$$\bigcap_{j \in A} \mathcal{R}'(Z_D | Z_j) \cap \mathcal{R}(Z_D)$$

(with $\mathcal{R}(Z_D)$ defined in (3.15)) is the achievable rate region for the omniscience constraint (3.13a) together with the rate constraints (3.16). $\bar{\rho}$ in (5.4a) is the minimum sum rate over this region. Since the above two rate constraints are separable, the total minimum sum rate is given by $\rho + \bar{\rho}$, which completes the proof.⁷

Achievability of C_S via omniscience:

We first argue that an optimal solution r_D to (5.4a) exists, and so the omniscience strategy is feasible. (An optimal solution $r_{V \setminus D \setminus S}$ to (5.3a) clearly exists.) As in (C.2), let

$$\mathcal{R}'(Z_D) := \{r_D \in \mathbb{R}^D \mid r(B) \geq H(Z_B | Z_{D \setminus B}) \forall B \subseteq D\}$$

which is the set of achievable rate tuples for encoding the components of Z_D independently so that they can be recovered from the codewords (without any side-information).

Proposition C.1 ([40]) $\mathcal{R}(Z_D)$ is the downward hull of $\mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D)$. \square

PROOF Since the entropy function is a normalized submodular function [26], $\mathcal{R}(Z_D)$ defines an extended polymatroid and

⁷As a side note, although the omniscience strategy here assumes non-interactive discussion, it can be shown as in [1] that the characterization of R_{CO} remains unchanged even if interactive discussion is allowed.

$\mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D)$ is the base of the polymatroid [40]. The result follows immediately from the fact that an extended polymatroid is a downward hull of its base. ■

It follows that $\mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D)$ is non-empty since its downward hull $\mathcal{R}(Z_D)$ is clearly non-empty. Furthermore,

$$r(D) = H(Z_D) \quad \forall r_D \in \mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D),$$

which is the maximum and minimum possible sum rates over $\mathcal{R}(Z_D)$ and $\mathcal{R}'(Z_D)$ respectively. An optimal solution to (5.4) exists because any $r_D \in \mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D)$ is a feasible solution, i.e., for all $j \in A$ and $B \subseteq D$,

$$\begin{aligned} r(B) &= r(D) - r(D \setminus B) \\ &\geq H(Z_D) - H(Z_{D \setminus B}) = H(Z_B | Z_{D \setminus B}), \end{aligned}$$

satisfying the constraint (5.4b).

It remains to show that the omniscience strategy achieves C_S in (3.9). Consider $r_{V \setminus D \setminus S}^*$ optimal to (5.3a) and any r_D^* optimal to (5.4a). By Proposition C.1, there exists a non-negative weight vector $r_D' \geq \mathbf{0}$ such that $r_D^* + r_D' \in \mathcal{R}(Z_D) \cap \mathcal{R}'(Z_D)$, which is therefore in $\mathcal{R}'(Z_D)$. By the usual source coding results [4], there exists (F, F_D') at rate $(r_{V \setminus S}^*, r_D')$ such that

$$\lim_{n \rightarrow \infty} \Pr(Z_D^n \neq \phi(F_D, F_D')) = 0$$

in addition to satisfying the omniscience constraints (3.13). It follows by Fano's inequality that the l.h.s. of the secrecy constraint (3.8) can be rewritten as

$$\begin{aligned} \liminf_{n \rightarrow \infty} \frac{1}{n} [\log |K| - H(K | F, Z_D^n)] \\ = \liminf_{n \rightarrow \infty} \frac{1}{n} [\log |K| - H(K | F, F_D')]. \end{aligned}$$

By [1, Lemma B.2], the r.h.s. can be made equal to 0 (satisfying (3.8)) with

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} \log |K| &\geq H(Z_{V \setminus S}) - r^*(V \setminus S) - r'(D) \\ &= H(Z_{V \setminus D \setminus S} | Z_D) - \overbrace{r^*(V \setminus D \setminus S)}^{=\rho} \\ &\quad + \underbrace{[H(Z_D) - r^*(D) - r'(D)]}_{=0}. \end{aligned}$$

This achieves the r.h.s. of (5.1) as desired.

2. Proofs of Theorem 5.2 and its Corollaries

PROOF (THEOREM 5.2) We will argue that for both the cases (i)-(ii), a capacity achieving scheme for the new scenario is a valid SK generation scheme for the original scenario and hence $C'_S \leq C_S$. In particular, if $C'_S = C_S$, then the capacity achieving schemes for the changed scenario will be capacity achieving for the original scenario as well, and hence $R_S \leq R'_S$.

Case (i): Consider turning an achievability scheme in the new scenario to that of the original scenario. To satisfy (3.5), the discussion by the new trusted helper can be performed by the original vocal active user. The original vocal active user can recover the key because the new silent active user can,

and so (3.7) holds. Observe that (3.8) continues to hold as the untrusted users remain unchanged.

Case (ii): The constraint on (3.5) becomes more stringent with the removal of a vocal helper, while the other constraints, namely, (3.7) and (3.8), remain unchanged. Hence, any capacity achieving scheme for the new scenario continues to be an SK generation scheme for the original one. ■

PROOF (COROLLARY 5.3) Suppose $C'_S = C_S$. The procedures (i) and (ii) correspond to the cases (i) and (ii) of Theorem 5.2, and so $R_S \leq R'_S$. Also, using (5.2) we have $R'_S \leq R'_{CO}$. Suppose $(\rho, \bar{\rho})$ becomes $(\rho', \bar{\rho}')$ in the new scenario. Note that, $\bar{\rho} = \bar{\rho}'$ if the sets (A, D) remain unchanged. We also have (5.1), that

$$\rho' = \rho - \underbrace{[H(Z_{(V \setminus D) \setminus S} | Z_D) - H(Z_{(V' \setminus D) \setminus S'} | Z_D)]}_{\beta},$$

by noting that $A \setminus S' = (V' \setminus D) \setminus S'$. Here,

$$\begin{aligned} \beta &= H(Z_{V \setminus S}) - H(Z_{V' \setminus S'}) \\ &= H(Z_{(S' \setminus S) \cup (V \setminus V')} | Z_{V' \setminus S'}) \geq 0. \end{aligned}$$

Hence, by (5.2), $R'_{CO} = \bar{\rho}' + \rho' = \bar{\rho} + \rho - \beta \leq \bar{\rho} + \rho = R_{CO}$, which completes the proof of (5.5). Furthermore, $R_S = R_{CO}$ happens only if $\beta = 0$, which is the same as (5.9). ■

PROOF (COROLLARY 5.4) Suppose, (5.7) holds. Then, by (5.8), every active user can recover U^n . By [1, Lemma B3], (3.8) holds for a choice of K as a function of U^n of rate $H(U | Z_D)$. Therefore, C_S can be achieved without public discussion, i.e., $R_S = 0$. Now, if (5.9) holds in addition, then (3.13) holds without discussion, i.e., $R_{CO} = 0$. Conversely, suppose that (5.9) fails, i.e., for some $j \in A$, $0 < H(Z_{V \setminus S} | Z_j) = H(Z_D | Z_j) + H(Z_{V \setminus S \setminus \{j\} \setminus D} | Z_j)$ holds. Then, either $H(Z_D | Z_j) > 0$, in which case $\bar{\rho} > 0$, or $H(Z_{V \setminus S \setminus \{j\} \setminus D} | Z_j) > 0$, in which case $\rho > 0$. In either case, $R_{CO} > 0$ by (5.2). ■

3. Proof of Theorem 5.3

The idea is to process the original source Z_V to $Z_V^{(q)}$ possibly with different choices of q at different times. We will show that (5.11) ensures that secrecy in the new scenario guarantees secrecy in the original scenario. On the other hand, (5.12) makes sure that the capacity does not diminish.

To proceed, divide the n -block of time instances into consecutive n_q -blocks for $q \in Q$, such that

$$\sum_{q \in Q} n_q = n \quad \text{and} \quad \lim_{n \rightarrow \infty} \frac{n_q}{n} = P_Q(q) \quad \forall q \in Q, \quad (C.3)$$

where, $P_Q(\cdot)$ is the distribution of some random variable Q taking values in a finite set Q . The source is processed block-by-block, with the source corresponding to the q -th block being processed to $Z_V^{(q)}$. Therefore, Z_V^n becomes $\bar{Z}_V := (Z_V^{(q)n_q} | q \in Q)$. There exists a public discussion F at the rate R'_{CO} for the active users to recover \bar{Z}_V , which can be argued using the *strong law of large numbers* and (C.3). By Lemma B3 of [1], a key K of rate equal to the r.h.s. of (5.12)

can be recovered by the active users, which satisfies (3.8) with Z_D replaced by \bar{Z}_D .

To complete the proof, we show that (3.8) is still valid with \bar{Z}_D . Recalling that $\bar{Z}_D = Z_D^n$, we have

$$\begin{aligned} \frac{1}{n} H(K|F, \bar{Z}_D) &= \frac{1}{n} H(K|F, Z_D^n) \\ &= \frac{1}{n} [H(K|F, \bar{Z}_D) - I(Z_D^n \wedge K|F, \bar{Z}_D)]. \end{aligned} \quad (\text{C.4})$$

Therefore, for some $\delta_n \rightarrow 0$,

$$\begin{aligned} I(Z_D^n \wedge K|F, \bar{Z}_D) &\leq I(Z_D^n \wedge \bar{Z}_{V \setminus D}, K|F, \bar{Z}_D) \\ &\stackrel{(a)}{\leq} I(Z_D^n \wedge \bar{Z}_{V \setminus D}|F, \bar{Z}_D) + n\delta_n \\ &\stackrel{(b)}{\leq} I(Z_D^n \wedge \bar{Z}_{V \setminus D}|\bar{Z}_D) + n\delta_n \\ &= \sum_{q \in Q} n_q I(Z_D \wedge Z_{V \setminus D}^{(q)}|\bar{Z}_D^{(q)}) + n\delta_n \\ &\stackrel{(c)}{=} n\delta_n. \end{aligned} \quad (\text{C.5})$$

(a) is by Fano's inequality because K is recoverable asymptotically from $\bar{Z}_{V \setminus D}$ given \bar{Z}_D . (b) is because F is determined by \bar{Z}_V . (c) follows directly from the assumption (5.11) in the theorem statement. Therefore, combining (C.4) and (C.5), we have $\frac{1}{n} H(K|F, \bar{Z}_D) \geq \frac{1}{n} H(K|F, \bar{Z}_D) - \delta_n$, which combined with (3.8) w.r.t. \bar{Z}_D gives us the desired result.

APPENDIX D PROOFS FOR SECTION VI

1. Proof of Shearer-Type Lemma

In this section, we prove a stronger version of Proposition 6.2 below:

Lemma D.1 *For any random vector (Z'_U, W') and $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$,*

$$I_\lambda(Z'_U|W') \geq \max_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) I(Z'_B \wedge Z'_{U \setminus B}|W') \quad (\text{D.1a})$$

$$I_\lambda(Z'_U|W') \leq \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) I(Z'_B \wedge Z'_{U \setminus B}|W') \quad (\text{D.1b})$$

which are the lower and upper bounds of the fractional partition information in terms of Shannon's mutual information. \square

Note that $I_\lambda(Z'_U|W') = 0$ implies the lower bound (D.1a) is zero, which implies (6.7). Conversely, $I_\lambda(Z'_U|W') = 0$ if the upper bound (D.1b) is zero, which is implied by (6.7).⁸

PROOF Without loss of generality, let $U := [m]$ for some integer $m > 1$, and assume the optimal solution to (D.1a) is $[l]$ for some $l \in [m]$. By definition (6.5),

$$I_\lambda(Z'_U|W') = \underbrace{H(Z'_U|W')}_{\textcircled{1}} - \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) \underbrace{H(Z'_B|Z'_{U \setminus B}, W')}_{\textcircled{2}}$$

⁸It also follows from Lemma D.1 that $I_\lambda(Z'_U|W') \rightarrow 0$ is equivalent to $\forall B \in \text{supp}(\lambda), I(Z'_B \wedge Z'_{U \setminus B}|W') \rightarrow 0$, which is not covered by Proposition 6.2 directly.

By the chain rule,

$$\begin{aligned} \textcircled{1} &= \sum_{i \in U} \overbrace{\sum_{B \in 2^U \setminus \{\emptyset, U\}: i \in B} \lambda(B)}^{= 1 \text{ by (6.1)}} H(Z'_i|Z'_{[i-1]}, W') \\ \textcircled{2} &= \sum_{i \in B} H(Z'_i|Z'_{[i-1] \cup (U \setminus B)}, W'). \end{aligned}$$

Exchanging the summations in $\textcircled{1}$, substituting both $\textcircled{1}$ and $\textcircled{2}$ back to the original expression and simplify using the definition of mutual information, we have

$$\begin{aligned} I_\lambda(Z'_U|W') &= \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) \sum_{i \in B} I(Z'_i \wedge Z'_{U \setminus B}|Z'_{[i-1]}, W') \\ &\stackrel{(a)}{\leq} \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) \sum_{i \in B} I(Z'_i \wedge Z'_{U \setminus B}|Z'_{[i-1] \cap B}, W') \\ &\stackrel{(b)}{=} \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) I(Z'_B \wedge Z'_{U \setminus B}|W') \end{aligned}$$

where (a) follows from the fact that conditioning does not increase entropy, and the equality holds if $[i-1] \subseteq B$; (b) follows from chain rule expansion. This gives the desired upper bound (D.1b). The lower bound (D.1a) follows from the equality case when $B = [l]$, and the fact that all the other terms in the sum are non-negative. \blacksquare

2. Proof of Lemma 6.1

Consider proving (6.8) first. By definition (6.5),

$$\begin{aligned} I_\lambda(Z'_U|W') - I_\lambda(Z''_U|W') &= \overbrace{H(Z'_U|W') - H(Z''_U|W')}^{\textcircled{1}} \\ &\quad - \sum_{B \in 2^U \setminus \{\emptyset, U\}} \lambda(B) \underbrace{\left[H(Z'_B|Z'_{U \setminus B}, W') - H(Z''_B|Z''_{U \setminus B}, W') \right]}_{\textcircled{2}} \end{aligned}$$

Note that by the definition of Z''_U , we have for $B \ni i$ that,

$$\textcircled{1} = \textcircled{2} = H(Z'_i|Z'_{U \setminus \{i\}}, W') - H(Z''_i|Z''_{U \setminus \{i\}}, W').$$

Since the value is independent of B , we have

$$\begin{aligned} I_\lambda(Z'_U|W') - I_\lambda(Z''_U|W') &= \textcircled{1} - \textcircled{1} \sum_{B \ni i} \lambda(B) - \sum_{B \not\ni i} \lambda(B) \textcircled{2} \\ &= - \sum_{B \not\ni i} \lambda(B) \textcircled{2} \end{aligned}$$

For $B \not\ni i$, it can be shown using standard arguments that

$$\begin{aligned} \textcircled{2} &= I(Z''_i \wedge Z'_B|Z'_{U \setminus B \setminus \{i\}}, W') - I(Z'_i \wedge Z'_B|Z'_{U \setminus B \setminus \{i\}}, W') \\ &\leq I(Z''_i \wedge Z'_B|Z'_{U \setminus B \setminus \{i\}}, W', Z'_i) \\ &\leq \underbrace{I(Z''_i \wedge Z'_{U \setminus \{i\}}|W', Z'_i)}_{\textcircled{3}}, \end{aligned}$$

the value of which is independent of B . Hence,

$$\begin{aligned} I_\lambda(Z'_U|W') - I_\lambda(Z''_U|W') &\geq -\textcircled{3} \sum_{B \not\ni i} \lambda(B) \\ &= -\textcircled{3} \left[\sum_B \lambda(B) - \sum_{B \ni i} \lambda(B) \right] \end{aligned}$$

which simplifies to $-\delta$ as desired by (6.1) and the fact that $Z_i'' = Y'$.

Consider proving (6.9). By definition (6.5),

$$\begin{aligned} I_\lambda(Z_U'|W') - I_\lambda(Z_U'|W', Y') \\ = \underbrace{I(Y' \wedge Z_U'|W')}_{\textcircled{4}} - \sum_B \lambda(B) \underbrace{I(Y' \wedge Z_B'|Z_{U \setminus B}', W')}_{\textcircled{5}} \end{aligned}$$

For $B \ni i$, we have by standard techniques that

$$\textcircled{5} \leq I(Y' \wedge Z_{U \setminus \{i\}}'|W', Z_i'),$$

the value of which is independent of B . Hence,

$$\sum_{B \ni i} \lambda(B) \textcircled{5} \leq \delta.$$

Hence, we have

$$I_\lambda(Z_U'|W') - I_\lambda(Z_U'|W', Y') + \delta \geq \textcircled{4} - \sum_{B \ni i} \lambda(B) \textcircled{5}$$

and so it suffices to prove that the r.h.s. is at least γ . By (6.1) again,

$$\begin{aligned} \textcircled{4} - \sum_{B \ni i} \lambda(B) \textcircled{5} &= \sum_{B \ni i} \lambda(B) [\textcircled{4} - \textcircled{5}] \\ &= \sum_{B \ni i} \lambda(B) I(Y' \wedge Z_{U \setminus B}'|W') \\ &\geq \sum_{B \ni i} \lambda(B) \max_{j \in U \setminus B} I(Y' \wedge Z_j'|W') \end{aligned}$$

which is at least γ as desired.

3. Proof of Theorem 6.1

We will show that for any C_S -achieving scheme,

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(K, F|\tilde{Z}_D) \geq J_{W, \lambda}(Z_U|Z_D) \quad (\text{D.2})$$

and so we have the desired lower bound (6.13) since

$$\begin{aligned} H(K, F|\tilde{Z}_D) &= H(F|\tilde{Z}_D) + H(K|F, \tilde{Z}_D) \quad \text{and} \\ \limsup_{n \rightarrow \infty} \frac{1}{n} H(K|F, \tilde{Z}_D) &\geq C_S = I_\lambda(Z_U|Z_D) \end{aligned}$$

by (3.8) and the assumption (6.12). To prove (D.2), we will rely on the following fundamental property of I_λ (6.5) for secret key agreement:

Lemma D.2 *If $C_S = I_\lambda(Z_U|Z_D)$ as in (6.12), then*

$$\lim_{n \rightarrow \infty} \frac{1}{n} I_\lambda(\tilde{Z}_U|K, F, \tilde{Z}_D) = 0 \quad (\text{D.3})$$

for any C_S -achieving scheme. \square

It follows that $L = (K, F)$ for any C_S -achieving scheme is a feasible solution to

$$C_{W, \lambda} := \inf \limsup_{n \rightarrow \infty} \frac{1}{n} H(L|\tilde{Z}_D) \quad \text{such that} \quad (\text{D.4a})$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} I_\lambda(\tilde{Z}_U|L, \tilde{Z}_D) = 0. \quad (\text{D.4b})$$

In other words,

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(K, F|\tilde{Z}_D) \geq C_{W, \lambda}.$$

and the proof is completed by showing that:

Lemma D.3

$$C_{W, \lambda} = J_{W, \lambda}(Z_U|Z_D), \quad (\text{D.5})$$

which is a single-letterization of (D.4). \square

PROOF (LEMMA D.2) We will show using the data processing inequalities in Lemma 6.1 that

$$\frac{1}{n} I_\lambda(\tilde{Z}_U|F, \tilde{Z}_D) \leq I_\lambda(Z_U|Z_D) \quad \text{and} \quad (\text{D.6a})$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \left\{ \log|K| - \left[I_\lambda(\tilde{Z}_U|F, \tilde{Z}_D) - I_\lambda(\tilde{Z}_U|K, F, \tilde{Z}_D) \right] \right\} \leq 0. \quad (\text{D.6b})$$

Then, for any C_S -achieving scheme,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \left[\log|K| - I_\lambda(\tilde{Z}_U|F, \tilde{Z}_D) \right] \geq 0$$

by (D.6a) and that the key rate is $C_S = I_\lambda(Z_U|Z_D)$ by assumption. Applying this to (D.6b) gives \leq in (D.3), and the reverse inequality follows from Proposition 6.2.

We first show (D.6a). Applying (6.9) with

$$Z_U' = \tilde{Z}_U, \quad Y' = F_{it}, \quad \text{and} \quad W' = (\tilde{Z}_D, \tilde{F}_{it})$$

for $i \in V \setminus S$ and $t \in [r]$ gives

$$I_\lambda(\tilde{Z}_U|\tilde{Z}_D, \tilde{F}_{it}, F_{it}) \leq I_\lambda(\tilde{Z}_U|\tilde{Z}_D, \tilde{F}_{it}), \quad (\text{D.7})$$

because $\gamma \geq 0$ and $\delta = 0$ in (6.9) as

$$\begin{aligned} I(Y' \wedge Z_{U \setminus \{i\}}'|W', Z_i') &\leq H(Y'|Z_i', W') \\ &= H(F_{it}|\tilde{Z}_i, \tilde{Z}_D, \tilde{F}_{it}) = 0 \end{aligned}$$

by (3.5). Applying (D.7) repeatedly for different (i, t) yields

$$\begin{aligned} I_\lambda(\tilde{Z}_U|\tilde{Z}_D) &\geq I_\lambda(\tilde{Z}_U|\tilde{Z}_D, F_{11}) \\ &\geq I_\lambda(\tilde{Z}_U|\tilde{Z}_D, F_{21}) \\ &\geq \dots \\ &\geq I_\lambda(\tilde{Z}_U|\tilde{Z}_D, F). \end{aligned} \quad (\text{D.8})$$

On the other hand, note that for all $B \subseteq U$, by (3.4),

$$\begin{aligned} H(\tilde{Z}_B|\tilde{Z}_D) &= H(Z_B^n, U_B|Z_D^n) \\ &= nH(Z_B|Z_D) + H(U_B), \end{aligned}$$

which gives

$$I_\lambda(\tilde{Z}_U|\tilde{Z}_D) = nI_\lambda(Z_U|Z_D) + I_\lambda(U_U)$$

for all $\lambda \in \Lambda(U, 2^U \setminus \{\emptyset, U\})$. Since $I_\lambda(U_U) = 0$ by (3.3) that U_i 's are mutually independent, the above equation implies $I_\lambda(\tilde{Z}_U|\tilde{Z}_D) = nI_\lambda(Z_U|Z_D)$. This together with (D.8) give the desired (D.6a).

To show (D.6b), we again apply (6.9) but with

$$Z_U' = \tilde{Z}_U, \quad Y' = K, \quad \text{and} \quad W' = (\tilde{Z}_D, F)$$

and any $i \in A \cap U$, which is feasible by the assumption $S \subsetneq A$ that there is at least one active vocal user and $U \supseteq V \setminus D \setminus S$ from (6.12). This gives

$$I_\lambda(\tilde{Z}_U | \tilde{Z}_D, F) \geq I_\lambda(\tilde{Z}_U | K, \tilde{Z}_D, F) + H(K | \tilde{Z}_D, F) - n\delta_n \quad (\text{D.9})$$

for some $\delta_n \rightarrow 0$ as $n \rightarrow \infty$, because

- the term δ in (6.9) goes to 0 because

$$I(Y' \wedge Z'_{U \setminus \{i\}} | Z'_i, W') \leq H(K | \tilde{Z}_i, \tilde{Z}_D, F) \leq n\delta'_n \quad (\text{D.10})$$

for some $\delta'_n \rightarrow 0$ as $n \rightarrow \infty$ by (3.7) and Fano's inequality;

- the term γ in (6.9) can be bounded as follow:

$$\begin{aligned} & \min_{B \in \text{supp}(\lambda): B \ni i} \max_{j \in U \setminus B} I(Y' \wedge Z'_j | W') \\ & \stackrel{(a)}{\geq} \min_{j \in A} I(Y' \wedge Z'_j | W') \\ & = \min_{j \in A} I(K \wedge \tilde{Z}_j | F, \tilde{Z}_D) \\ & = \min_{j \in A} [H(K | F, \tilde{Z}_D) - H(K | \tilde{Z}_j, F, \tilde{Z}_D)] \\ & \stackrel{(b)}{\geq} \min_{j \in A} H(K | F, \tilde{Z}_D) - n\delta'_n \end{aligned}$$

where (a) is due to $(U \setminus B) \cap A \neq \emptyset, \forall B \in 2^U \setminus \{\emptyset, U\}$,
(b) is by (D.10) (with j in place of i).

(D.9) implies (D.6b) by (3.8) as desired. Although not essential for the proof of the lemma here, the reverse inequality \geq of (D.6b) also holds more generally by the definition of I_λ :

$$\begin{aligned} I_\lambda(\tilde{Z}_U | F, \tilde{Z}_D) - I_\lambda(\tilde{Z}_U | K, F, \tilde{Z}_D) \\ = H(K | F, \tilde{Z}_D) - \sum_B \lambda(B) H(K | \tilde{Z}_{U \setminus B}, F, \tilde{Z}_D) \\ \leq \log |K|. \end{aligned}$$

Hence, (D.6b) is indeed satisfied with equality. ■

PROOF (LEMMA D.3) We single-letterize $C_{W,\lambda}$ as in [32]:

$$\begin{aligned} H(L | \tilde{Z}_D) & \geq I(Z_U^n \wedge L | \tilde{Z}_D) \\ & = H(Z_U^n | \tilde{Z}_D) - H(Z_U^n | \tilde{Z}_D, L) \\ & = \sum_{t=1}^n H(Z_{Ut} | Z_{Dt}) - \sum_{t=1}^n H(Z_{Ut} | Z_U^{t-1}, \tilde{Z}_D, L) \\ & = \sum_{t=1}^n H(Z_{Ut} | Z_{Dt}) - \sum_{t=1}^n H(Z_{Ut} | Z_U^{t-1}, \tilde{Z}_D, L, Z_{Dt}) \\ & = nI(Z_{UJ} \wedge W_J | Z_{DJ}) \end{aligned} \quad (\text{D.11})$$

where J is the usual time-sharing random variable uniformly distributed over $[n]$ and independent of (Z_U, \tilde{Z}_D, L) , and

$$W_J := (J, Z_U^{J-1}, L, \tilde{Z}_D).$$

We can also bound I_λ in the constraint (D.4b) of $C_{W,\lambda}$:

$$I_\lambda(\tilde{Z}_U | L, \tilde{Z}_D) \geq \underbrace{I_\lambda(Z_U^n | L, \tilde{Z}_D)}_{\textcircled{1}}$$

by the data processing inequality (6.8) since Z_i^n is determined by \tilde{Z}_i . By definition (6.5)

$$\textcircled{1} = \underbrace{H(Z_U^n | L, \tilde{Z}_D)}_{\textcircled{2}} - \sum_B \lambda(B) \underbrace{H(Z_B^n | Z_{U \setminus B}^n, L, \tilde{Z}_D)}_{\textcircled{3}} \quad (\text{D.12})$$

Using the fact that $\tilde{Z}_D = Z_D^n$, the r.h.s. can be further expanded as follows:

$$\begin{aligned} \textcircled{2} & = \sum_{t=1}^n H(Z_{Ut} | Z_U^{t-1}, L, Z_D^n) \\ & = \sum_{t=1}^n H(Z_{Ut} | Z_U^{t-1}, L, Z_D^n, Z_{Dt}) \\ & = nH(Z_{UJ} | W_J, Z_{DJ}) \\ \textcircled{3} & = \sum_{t=1}^n H(Z_{Bt} | Z_B^{t-1}, Z_{U \setminus B}^n, L, Z_D^n, Z_{Dt}) \\ & \leq \sum_{t=1}^n H(Z_{Bt} | Z_U^{t-1}, Z_{\{U \setminus B\}t}, L, Z_D^n, Z_{Dt}) \\ & = nH(Z_{BJ} | W_J, Z_{\{U \setminus B\}J}, Z_{DJ}) \end{aligned}$$

Altogether, we have the inequality

$$I_\lambda(Z_{UJ} | W_J, Z_{DJ}) \leq \frac{1}{n} I_\lambda(\tilde{Z}_U | L, \tilde{Z}_D). \quad (\text{D.13})$$

Similar to the arguments in the proof of Theorem 4.1 in Appendix B-1, by (D.11) and (D.13), and the fact that Z_{UJ} has the same distribution as Z_U , we have

$$\begin{aligned} C_{W,\lambda} & \geq H(Z_U | Z_D) - \lim_{\delta \rightarrow 0} \Gamma(\delta) \quad \text{where} \\ \Gamma(\delta) & := \sup_{P_{W|Z_{U \cup D}}: I_\lambda(Z_U | W, Z_D) \leq \delta} H(Z_U | Z_D, W). \end{aligned} \quad (\text{D.14})$$

(In fact, the above inequality is satisfied with equality.⁹) Note that

$$H(Z_U | Z_D) - \Gamma(0) = J_{W,\lambda}(Z_U | Z_D) \quad (\text{D.15})$$

and so the proof is completed by showing that $\Gamma(\delta)$ is continuous at $\delta = 0$. To show this, we will prove the following support-type lemma that extends Proposition 6.3, following essentially the same argument as in [32]. ■

Lemma D.4 *It is admissible to impose in (D.14) that*

$$|W| \leq \begin{cases} |Z_{U \cup D}| + 1 & \delta > 0 \\ |Z_{U \cup D}| & \delta = 0, \end{cases} \quad (\text{D.16})$$

and so sup in (D.14) can be replaced by max and $\Gamma(\delta)$ is continuous in δ .¹⁰ □

PROOF (LEMMA D.4) Pick any $z'_{U \cup D} \in Z_{U \cup D}$, and define S as the set of all possible vectors of values for

$$\begin{aligned} & (H(Z_U | Z_D, W = w), I_\lambda(Z_U | Z_D, W = w), \\ & P_{Z_{U \cup D} | W=w}(z_{U \cup D}) \mid z_{U \cup D} \in Z_{U \cup D} \setminus \{z'_{U \cup D}\}). \end{aligned}$$

⁹The reverse inequality holds by the fact W^n i.i.d. generated according to the solution $P_{W|Z_{U \cup D}}$ to (D.14) is a feasible solution to (D.4).

¹⁰As in [32], it is also possible to argue that $\Gamma(\delta)$ is non-decreasing and concave in δ .

There is a one-to-one mapping between the choice of $P_{Z_{U \cup D}|W=w}$ and the choice of $\mathbf{v}(w) \in \mathcal{S}$, noting that

$$P_{Z_{U \cup D}|W=w}(\mathbf{z}'_{U \cup D}) = 1 - \sum_{\mathbf{z} \in Z_{U \cup D} \setminus \{\mathbf{z}'_{U \cup D}\}} P_{Z_{U \cup D}|W=w}(\mathbf{z}_{U \cup D}).$$

Thus, a feasible solution to (D.14) corresponds to a choice of a set W , a distribution P_W over W , and a vector $\mathbf{v}(w)$ for every $w \in W$, such that

$$\sum P_W(w) \mathbf{v}(w) = (H(Z_U|Z_D, W), I_\lambda(Z_U|Z_D, W)), \quad (\text{D.17})$$

$$P_{Z_{U \cup D}|W}(\mathbf{z}_{U \cup D}) \mid \mathbf{z}_{U \cup D} \in Z_{U \cup D} \setminus \{\mathbf{z}'_{U \cup D}\}. \quad (\text{D.18})$$

By the Fenchel-Eggleston-Carathéodory theorem [41], it is admissible to choose $|W|$ equal to the length of $\mathbf{v}(w)$ plus 1, i.e., $|Z_{U \cup D}| + 1$ as desired in (D.16) for $\delta \geq 0$. If $\delta = 0$, i.e., one requires $I_\lambda(Z_U|Z_D, W) = 0$, then $I_\lambda(Z_U|Z_D, W = w) = 0$ for all $w \in W$ since I_λ is non-negative by Proposition 6.2. In other words, the constraint is on individual choice of $P_{Z_{U \cup D}|W=w}$ and so we can redefine \mathcal{S} without having $I_\lambda(Z_U|Z_D, W = w)$ as a component of $\mathbf{v}(w)$, i.e., which gives the smaller bound in (D.16).

Suppose there is a sequence in k of choices of $(P_{W_k}, P_{Z_{U \cup D}|W_k})$ that attains $\Gamma(\delta)$ in the limit as $k \rightarrow \infty$ while satisfying the constraint in (D.14), i.e.,

$$I_\lambda(Z_U|Z_D, W_k) \leq \delta$$

By imposing (D.16) such that W is finite with size independent of k , the feasible choices of $(P_{W_k}, P_{Z_{U \cup D}|W_k})$ form a compact set. Hence, there exists a subsequence $\{k_j\}_{j=1}^\infty$ such that

$$P_W = \lim_{j \rightarrow \infty} P_{W_{k_j}} \text{ and } P_{Z_{U \cup D}|W} = \lim_{j \rightarrow \infty} P_{Z_{U \cup D}|W_{k_j}}. \quad (\text{D.19})$$

By the continuity of entropy [4], we also have

$$I_\lambda(Z_U|Z_D, W) = \lim_{j \rightarrow \infty} I_\lambda(Z_U|Z_D, W_{k_j}), \text{ and} \quad (\text{D.20a})$$

$$H(Z_U|Z_D, W) = \lim_{j \rightarrow \infty} H(Z_U|Z_D, W_{k_j}). \quad (\text{D.20b})$$

Note that the r.h.s. of (D.20a) is upper bounded by δ since each term in the limit is. Furthermore, the r.h.s. of (D.20b) attains $\Gamma(\delta)$ by assumption. Hence, the supremum in (D.14) is achieved by the above choice of W , i.e., the sup in (D.14) can be replaced by max.

Consider proving the continuity of $\Gamma(\delta)$. Consider any sequence $\{\delta_k\}_{k=1}^\infty$ such that $\delta_k > \delta$ and $\delta_k \downarrow \delta$ as $k \uparrow \infty$. Since $\Gamma(\delta)$ is non-decreasing in δ , we have

$$\Gamma(\delta) \leq \lim_{k \rightarrow \infty} \Gamma(\delta_k). \quad (\text{D.21})$$

Let $(P_{W_k}, P_{Z_{U \cup D}|W_k})$ be the optimal solution for $\Gamma(\delta_k)$. Then, as argued previously, $(P_W, P_{Z_{U \cup D}|W})$ exists satisfying (D.19) and (D.20) for some subsequent $\{k_j\}_{j=1}^\infty$. Furthermore, the r.h.s. of (D.20a) is equal to $\lim_{k \rightarrow \infty} \delta_k = \delta$, and so W is a feasible solution to (D.14). The l.h.s. of (D.20b) is therefore upper bounded by $\Gamma(\delta)$ and so

$$\Gamma(\delta) \geq \lim_{k \rightarrow \infty} \Gamma(\delta_k),$$

which is satisfied with equality by (D.21), implying that $\Gamma(\delta)$ is continuous in δ . ■

4. Proof of Theorem 6.2

(6.15a) follows from Theorem 6.1 directly since $C_S = I_{\lambda^*}(Z_V)$ for all $\lambda^* \in \Lambda^*(A, Z_V)$. To show (6.15b), choose $\lambda^* \in \Lambda^*(A, Z_V)$ such that

$$\text{supp}(\lambda^*) = \bigcup_{\lambda' \in \Lambda^*(A, Z_V)} \text{supp}(\lambda').$$

This is possible, for instance, by choosing λ^* as the average of the extreme elements in $\Lambda^*(A, Z_V)$, which are the vertices of the feasible set in (6.6), and so there are only a finite number of them by (6.1). Let W be the optimal solution to $J_{W, \lambda^*}(Z_V)$, and consider $\lambda \in \Lambda(V, \mathcal{H})$ with \mathcal{H} defined in (6.14), we then have

$$\begin{aligned} J_{W, \lambda^*}(Z_V) &= I(Z_V \wedge W) \\ &= H(Z_V) - H(Z_V|W) \\ &\stackrel{(a)}{\geq} H(Z_V) - \sum_{B \in \mathcal{H}} \lambda(B) H(Z_B|W) \\ &\stackrel{(b)}{=} H(Z_V) - \sum_{B \in \mathcal{H}} \lambda(B) H(Z_B|Z_{V \setminus B}, W) \\ &\geq H(Z_V) - \sum_{B \in \mathcal{H}} \lambda(B) H(Z_B|Z_{V \setminus B}) \end{aligned}$$

which gives $I_\lambda(Z_V)$ as desired by (6.5). The inequality (a) is because of the Shearer-type Lemma [39] stated in a slightly different form than Proposition 6.2:

$$\begin{aligned} \sum_B \lambda(B) H(Z_B|W) &= \sum_B \lambda(B) \sum_{i \in B} H(Z_i|Z_{[i-1] \cap B}, W) \\ &\geq \sum_B \lambda(B) \sum_{i \in B} H(Z_i|Z_{[i-1]}, W) \\ &= \sum_{i \in V} \sum_{B \ni i} \lambda(B) H(Z_i|Z_{[i-1]}, W) \\ &= \sum_{i \in V} H(Z_i|Z_{[i-1]}, W) \\ &= H(Z_V|W). \end{aligned}$$

The equality (b) is because the definition of $J_{W, \lambda^*}(Z_V)$ requires $I_{\lambda^*}(Z_V|W) = 0$, which by Proposition 6.2, results in $I(Z_B \wedge Z_{V \setminus B}|W) = 0$ for all $B \in \text{supp}(\lambda^*)$, and hence, for all $B \in \mathcal{H}$.

5. Proofs for Section VI-D

PROOF (PROPOSITION 6.4) Applying Theorem 5.1 to the current case $S \subsetneq A = V$, (5.1) becomes

$$C_S = H(Z_{V \setminus S}) - R_{CO}, \quad (\text{D.22})$$

where $R_{CO} = \rho = \min_{r(V \setminus S)} r(V \setminus S)$ subject to the constraints

$$r(B) \geq H(Z_B|Z_{(V \setminus S) \setminus B}) \quad \forall B \subsetneq V \setminus S : B \neq \emptyset \quad (\text{D.23a})$$

$$r(V \setminus S) \geq H(Z_{V \setminus S}|Z_i) \quad \forall i \in S, \quad (\text{D.23b})$$

where we have used a similar argument as in the proof of Corollary 5.1 to derive (D.23a). Note also that the set of constraints are equivalent to the those in Corollary 5.2 but

stated in a convenient form for the current proof. We proceed to prove (6.18a) and hence assume $|V \setminus S| = 1$. Observe that this condition renders (D.23a) obsolete and hence using (D.22) we have $C_S = H(Z_{V \setminus S}) - \max_{i \in S} H(Z_{V \setminus S} | Z_i) = \alpha$ as desired.

To complete the proof of Proposition 6.4 we consider the case when $|V \setminus S| > 1$. Again, we shall prove this in a case by case basis. First, consider the case when (D.23b) are redundant, and hence $R_{CO} \geq \max_{i \in S} H(Z_{V \setminus S} | Z_i)$. Also, observe that since $R_{CO} = \min_{r_{V \setminus S}} r(V \setminus S)$, where $r_{V \setminus S}$ is constrained by the first set of constraints in (D.23a), we have $H(Z_{V \setminus S}) - R_{CO} = I(Z_{V \setminus S})$ using Proposition 4.2. Therefore, using (D.22), we have $C_S = I(Z_{V \setminus S})$. Also, from the fact that $R_{CO} \geq \max_{i \in S} H(Z_{V \setminus S} | Z_i)$, we have $C_S = H(Z_{V \setminus S}) - R_{CO} \leq \alpha$, and hence (6.18b) is satisfied. We finish the proof by looking at the remaining case, i.e., when there exists some $i \in S$ such that (D.23b) is not redundant. An immediate consequence of this is $R_{CO} = H(Z_{V \setminus S} | Z_i)$ and hence using (D.22) we have $C_S = \alpha$. Also, defining $R'_{CO} = \min_{r_{V \setminus S}} r(V \setminus S)$, where $r_{V \setminus S}$ is constrained by (D.23a), we see that $R_{CO} \geq R'_{CO}$. Therefore, using Proposition 4.2, we have $I(Z_{V \setminus S}) \geq H(Z_{V \setminus S}) - R_{CO} = C_S$. Hence, we have $C_S = \min\{\alpha, I(Z_{V \setminus S})\}$ as desired. ■

PROOF (THEOREM 6.4) We first consider the case when the conditions for (6.20a) hold. The proof is carried out by exactly following the same steps as in the proof of Theorem 4.1 with the choice $\mathcal{P} = \mathcal{P}^*(Z_{V \setminus S})$. This is possible as in this case $C_S = I(Z_{V \setminus S})$ by (6.18b). Similarly, we prove the result for the case when the conditions for (6.20b) hold, by using $C_S = I(Z_{V \setminus S} \wedge Z_i)$, for some $i \in S^*$, which follows from (6.18a).

For the remaining case when $|V \setminus S| > 1$ and $\alpha = I(Z_{V \setminus S})$, we observe using (6.18b) that every $i \in S^*$ satisfies

$$C_S = I_{\mathcal{P}^*}(Z_{V \setminus S}) = I(Z_{V \setminus S} \wedge Z_i). \quad (\text{D.24})$$

Corollary 5.3 of [9], says that there exists some $\theta \in (0, 1)$ which satisfies $I_{\mathcal{P}}(Z_{(V \setminus S) \cup \{i\}}) = \theta I_{\mathcal{P}^*}(Z_{V \setminus S}) + (1 - \theta)I(Z_{V \setminus S} \wedge Z_i)$, with $\mathcal{P} = \mathcal{P}^*(Z_{V \setminus S}) \cup \{i\}$. Hence, using (D.24), we have $C_S = I_{\mathcal{P}}(Z_{(V \setminus S) \cup \{i\}})$ for every $i \in S^*$. The result now follows by proceeding along the same steps as in the proof of Theorem 4.1, with the choice $\mathcal{P} = \mathcal{P}^*(Z_{V \setminus S}) \cup \{i\}$, for any $i \in S^*$. ■

PROOF (THEOREM 6.5) The proof technique is similar to the proof of Theorem 4.2. We use the hypothesis of Theorem 6.5 to show that the lower bound to R_S obtained in Theorem 6.4 evaluates to R_{CO} . This, in conjunction with the trivial upper bound $R_S \leq R_{CO}$, gives us the result.

We first observe that the conditions in (i) imply that $J_{D, \mathcal{P}^*}(Z_{V \setminus S}) = H(Z_{V \setminus S})$. Hence, via (6.20a) and the inequality $J_{W, \mathcal{P}^*}(Z_{V \setminus S}) \geq J_{D, \mathcal{P}^*}(Z_{V \setminus S})$, we have $R_S \geq H(Z_{V \setminus S}) - I(Z_{V \setminus S}) = R_{CO}$.

Next we consider the case when the conditions in (ii) hold. Therefore, there exists $i \in S^*$ satisfying $J_{D, \{V \setminus S, \{i\}\}}(Z_{V \setminus S}, Z_i) = H(Z_{V \setminus S}, Z_i) - H(Z_i | Z_{V \setminus S}) =$

$H(Z_{V \setminus S})$. Using (D.22) and Proposition 6.4, the bound in (6.20b) evaluates to $R_S \geq R_{CO}$.

To complete the proof, we look at the scenario described in (iii). Observe that there exists $i \in S^*$, such that $J_{D, \mathcal{P}^*(Z_{V \setminus S}) \cup \{i\}}(Z_{(V \setminus S) \cup \{i\}}) = H(Z_{V \setminus S}, Z_i) - \sum_{C \in \mathcal{P}^*(Z_{V \setminus S})} H(Z_C | Z_{(V \setminus S) \setminus C}, Z_i) - H(Z_i | Z_{V \setminus S}) = H(Z_{V \setminus S})$. Hence, the lower bound to R_S in (6.20c) evaluates to R_{CO} by (6.18b) and (D.22). Therefore, we have $R_S = R_{CO}$ as required. ■

6. Proofs for Section VI-E

PROOF (PROPOSITION 6.5) Choose any vocal active user $j \in A \cap (V \setminus S)$. Observe that by (3.7), it is admissible to choose the secret key $K = \theta_j(\tilde{Z}_j, F)$ for some function θ_j . Assume there is a hyperedge e' such that $\xi(e') \subseteq S$. Then, the sequence of random variables $X_{e'}^n$ associated with the hyperedge e' is independent of $(K, F, (X_e^n | e \in E \setminus \{e'\}), U_{V \setminus S})$. This is because $X_{e'}$ is not observed by any vocal user, including j , who generate K, F entirely from $((X_e^n | e \in E \setminus \{e'\}), U_{V \setminus S})$. Similarly, it can be argued that $X_{e'}^n$ does not play any part in recovering $Z_{V \setminus S}^n$, as it is independent of X_e^n . Therefore, removing the hyperedge e' does not affect C_S, R_S and R_{CO} . ■

PROOF (THEOREM 6.6) Proposition 6.5 ensures it is enough to prove the results for hypergraphs satisfying (6.21). Observe that (6.22a) follows directly from (6.20a). We only need to verify the other two scenarios.

We begin by arguing the following claim, that $I(Z_j \wedge Z_{(V \setminus S) \cup S'}) = \alpha$, for all $j \in S^*$, and all $S' \subseteq S^* \setminus \{j\}$. First, assume to the contrary that we have a strict inequality ($>$) instead of an equality for some $i \in S^*$ and some $S' \subseteq S^* \setminus \{i\}$. Then, there exists a hyperedge $e' \in E$ that contributes to $I(Z_j \wedge Z_{(V \setminus S) \cup S'}) = H(X_{e'})$, but not to $I(Z_i \wedge Z_{V \setminus S}) = H(X_{e''})$, i.e., $e' \in E' \setminus E''$ and $E' \supseteq E''$. It immediately implies that $j \in \xi(e')$ and $\xi(e') \subseteq S$, which violates (6.21). Hence, we must have $I(Z_j \wedge Z_{(V \setminus S) \cup S'}) = \alpha$, for all $j \in S^*$ and all $S' \subseteq S^* \setminus \{j\}$.

Using the above claim, we proceed to prove (6.22c). Consider any $j \in S^*$, and observe that $\alpha = I(Z_{V \setminus S} \wedge Z_j) = I_{\mathcal{P}^*}(Z_{V \setminus S})$, using the hypothesis of (6.22c). Now, using Corollary 5.3 of [9], there exists $\theta \in (0, 1)$ such that $I_{\mathcal{P}^*(Z_{V \setminus S}) \cup \{j\}}(Z_{(V \setminus S) \cup \{j\}}) = \theta I_{\mathcal{P}^*}(Z_{V \setminus S}) + (1 - \theta)I(Z_{V \setminus S} \wedge Z_j) = \alpha$. We can continue with this process inductively to show that $I_{\mathcal{P}^*(Z_{V \setminus S}) \cup \{\{i\} | i \in S^*\}}(Z_{(V \setminus S) \cup S^*}) = \alpha = C_S$. Using this, one can proceed along similar steps as in the proof of Theorem 4.1 to obtain (6.22c).

The proof of (6.22b) follows using a similar inductive argument and we omit the details. ■

PROOF (THEOREM 6.7) To begin with, we restrict our attention to hypergraphs satisfying (6.21). This is because of Proposition 6.5 and the fact that none of the entropy terms in (i)-(iii) are affected by the removal of some hyperedge e satisfying $\xi(e) \subseteq S$.

We omit the proof of the fact that $R_S = R_{CO}$ if the required condition from (i)-(iii) hold, by noting that the proof follows from Theorem 6.6 by the same steps as in the proof

of Theorem 6.5. We focus on proving the fact that $R_S = R_{CO}$ implies that the required condition from (i)-(iii) hold. We proceed according to a case by case basis.

Case I: $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < \alpha$.

We assume that (i) does not hold. We will show that $R_S < R_{CO}$. Then, there exists $e' \in E$ such that $\xi(e') \setminus S \subseteq C$, for some $C \in \mathcal{P}^*(V \setminus S)$. We use the idea of *decremental secret key agreement* as in [37] to reduce $H(X_{e'})$ by an amount $\epsilon \in (0, \alpha - I(Z_{V \setminus S}))$. Whereas, this operation does not affect $I(Z_{V \setminus S})$, we note that α changes by at most ϵ , thereby keeping C_S unaffected. However, $H(Z_{V \setminus S})$ does decrease by ϵ , and the fact that C_S remains unchanged implies that R_{CO} reduces by ϵ using (D.22). Thus, we must have R_S being strictly less than the R_{CO} before the reduction by ϵ .

Case II: $|V \setminus S| = 1$ or, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$.

Here, we drop the case when $|V \setminus S| = 1$ as the condition holds by default.

Again, assume (ii) does not hold. Then, there exists a hyperedge $e' \in E$ such that $\xi(e') \subseteq (V \setminus S^*)$. We can reduce the entropy of $X_{e'}$ by some $\epsilon > 0$ small enough without affecting the secrecy capacity using decremental secret key agreement of [37]. If $|V \setminus S| = 1$, we can choose any $\epsilon \in (0, \min_{i \in S/S^*} I(Z_{V \setminus S} \wedge Z_i) - \alpha)$ as the reduction in entropy will not affect the set S^* of optimal solutions and therefore α . In the other case $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$, we impose an additional constraint that $\epsilon < I(Z_{V \setminus S}) - \alpha$. Then, α remains unaffected after the reduction in entropy, whereas $I(Z_{V \setminus S})$ decreases by at most ϵ . Thus, C_S remains unchanged. Moreover, the fact that (6.21) holds implies $H(Z_{V \setminus S})$ reduces by ϵ , and so does R_{CO} using (D.22). Therefore, we must have $R_S < R_{CO}$ before reduction.

Case III: $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = \alpha$

Assume (iii) is invalid and hence, there exists $e' \in E$ such that $\xi(e') \subseteq C$ for some $C \in \mathcal{P}^*(Z_{V \setminus S})$. We reduce the entropy of X_e by some amount of $\epsilon > 0$. While α remains unaffected by the operation, the decremental secret key agreement detailed in [37] ensures that choosing ϵ sufficiently small not affect $I(Z_{V \setminus S})$ either. Thus, C_S is unaffected. However, clearly $H(Z_{V \setminus S})$ reduces by ϵ and so does R_{CO} . Hence, $R_S < R_{CO}$ before reduction as required. ■

APPENDIX E

PROOF FOR SECTION VII

1. Proof of Proposition 7.1

To prove the desired result, we will make use of the following independence relation satisfied by the private source:

$$0 = I(Z_1 \wedge Z_2) = I(Z_3 \wedge Z_{\{1,2,4\}}) = I(Z_3 \wedge Z_{\{1,2,5\}}). \quad (\text{E.1})$$

For this specific example, assume the discussion order is

$$3 \rightarrow 4 \rightarrow 5 \rightarrow 1 \rightarrow 2. \quad (\text{E.2})$$

The desired conclusion will be proved by showing the stronger result that

$$\limsup_{n \rightarrow \infty} \frac{1}{n} [H(F_{\{1,2,4,5\}}) - 3H(K)] \geq 0 \quad (\text{E.3})$$

which implies $R_S \geq 3C_S = 3 = R_{CO}$ as desired.

To prove the above, define

$$a_t := I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_V^t) - I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_V^{t-1}) \quad (\text{E.4a})$$

$$b_t := I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,4\}} | F_V^t) - I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) \quad (\text{E.4b})$$

$$c_t := I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,5\}} | F_V^t) - I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,5\}} | F_V^{t-1}) \quad (\text{E.4c})$$

By definition of (E.4), we have

$$\begin{aligned} & \sum_{t=1}^r (a_t + b_t + c_t) \\ &= I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F) + I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,4\}} | F) + I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,5\}} | F) \\ &\geq 3H(K) - 3n\delta_n \end{aligned}$$

for some $\delta_n \rightarrow 0$ as $n \rightarrow \infty$. Here, the inequality follows from the recoverability (3.7) and secrecy (3.8) requirement, for instance, $I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F) \geq I(\tilde{Z}_1, K \wedge \tilde{Z}_2, K | F) - \frac{n\delta_n}{2} \geq H(K) - n\delta_n$. Then, it suffices to show that

$$H(F_{\{1,2,4,5\}}) \geq \sum_{t=1}^r (a_t + b_t + c_t). \quad (\text{E.5})$$

To achieve this, we will bound a_t, b_t and c_t one by one. We first bound a_t as follows:

$$\begin{aligned} a_t &\leq I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_V^t) - I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_V^{t-1}) + I(\tilde{Z}_2 \wedge F_{Vt} | F_V^{t-1}) \\ &= I(\tilde{Z}_2 \wedge F_{Vt} | \tilde{Z}_1, F_V^{t-1}) \\ &\leq I(\tilde{Z}_2 \wedge F_{Vt} | \tilde{Z}_1, F_V^{t-1}) + I(\tilde{Z}_1 \wedge F_{Vt} | F_V^{t-1}) \\ &= I(\tilde{Z}_{\{1,2\}} \wedge F_{Vt} | F_V^{t-1}) \end{aligned}$$

We then bound b_t as follows:

$$\begin{aligned} b_t &\stackrel{(a)}{=} I(F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}, \tilde{Z}_3) - I(F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) \\ &\stackrel{(b)}{=} I(F_{Vt} \wedge \tilde{Z}_{\{1,2,3,4\}} | F_V^{t-1}) - I(F_{Vt} \wedge \tilde{Z}_3 | F_V^{t-1}) \\ &\quad - I(F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) \\ &\stackrel{(c)}{\leq} H(F_{Vt} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}) - I(F_{Vt} \wedge \tilde{Z}_3 | F_V^{t-1}) \\ &\stackrel{(d)}{=} H(F_{3t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}) + H(F_{4t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}, F_{3t}) \\ &\quad + H(F_{5t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}, F_{\{3,4\}t}) - I(F_{Vt} \wedge \tilde{Z}_3 | F_V^{t-1}) \\ &\stackrel{(e)}{=} H(F_{3t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}) + H(F_{5t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}, F_{\{3,4\}t}) \\ &\quad - I(F_{Vt} \wedge \tilde{Z}_3, F_{3t} | F_V^{t-1}) \\ &\stackrel{(f)}{\leq} H(F_{3t} | F_V^{t-1}, \tilde{Z}_{\{1,2\}}) + H(F_{5t} | F_V^{t-1}, \tilde{Z}_{\{1,2\}}, F_{\{3,4\}t}) \\ &\quad - H(F_{3t} | F_V^{t-1}) \end{aligned}$$

where (a) is due to the fact that

$$\begin{aligned} & I(\tilde{Z}_3, F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) \\ &= I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) + I(F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}, \tilde{Z}_3) \\ &= I(F_{Vt} \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}) + I(\tilde{Z}_3 \wedge \tilde{Z}_{\{1,2,4\}} | F_V^{t-1}), \end{aligned}$$

(b) is due to the chain rule expansion, (c) is due to the fact that

$$I(F_{Vt} \wedge \tilde{Z}_{\{1,2,3,4\}} | F_V^{t-1}) \leq H(F_{Vt} | F_V^{t-1}),$$

(d) is due to the chain rule expansion and the fact that

$$H(F_{[2]t} | F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}, F_{\{3,4,5\}t}) = 0$$

by (3.5) with discussion order (E.2). Similarly, (e) follows from (3.5) with discussion order (E.2) that

$$\begin{aligned} H(F_{4t}|F_V^{t-1}, \tilde{Z}_{\{1,2,4\}}, F_{3t}) &= 0 \\ I(F_{Vt} \wedge \tilde{Z}_3|F_V^{t-1}) &= I(F_{Vt} \wedge \tilde{Z}_3, F_{3t}|F_V^{t-1}). \end{aligned}$$

(f) is because

$$\begin{aligned} I(F_{Vt} \wedge \tilde{Z}_3, F_{3t}|F_V^{t-1}) \\ &= I(F_{Vt} \wedge F_{3t}|F_V^{t-1}) + I(F_{Vt} \wedge \tilde{Z}_3|F_V^{t-1}, F_{3t}) \\ &\geq H(F_{3t}|F_V^{t-1}) \end{aligned}$$

Following similar steps as above, c_t is also upper bounded by

$$\begin{aligned} c_t &\leq H(F_{\{3,4\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2,5\}}) - H(F_{3t}|F_V^{t-1}) \\ &\quad + H(F_{5t}|F_V^{t-1}, \tilde{Z}_{\{1,2,5\}}, F_{\{3,4\}t}) \\ &\leq H(F_{\{3,4\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) - H(F_{3t}|F_V^{t-1}) \end{aligned}$$

Therefore, we have $a_t + b_t + c_t$

$$\begin{aligned} &\leq I(\tilde{Z}_{\{1,2\}} \wedge F_{Vt}|F_V^{t-1}) + H(F_{3t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \\ &\quad + H(F_{5t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}, F_{\{3,4\}t}) + H(F_{\{3,4\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \\ &\quad - 2H(F_{3t}|F_V^{t-1}) \\ &\stackrel{(a)}{\leq} H(F_{Vt}|F_V^{t-1}) - H(F_{3t}|F_V^{t-1}) \\ &= H(F_{\{1,2,4,5\}t}|F_V^{t-1}, F_{3t}). \end{aligned}$$

where (a) is because

$$\begin{aligned} &I(\tilde{Z}_{\{1,2\}} \wedge F_{Vt}|F_V^{t-1}) \\ &= H(F_{Vt}|F_V^{t-1}) - H(F_{Vt}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \\ &= H(F_{Vt}|F_V^{t-1}) - H(F_{\{3,4,5\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \\ &\quad - H(F_{\{1,2\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}, F_{\{3,4,5\}t}) \\ &= H(F_{Vt}|F_V^{t-1}) - H(F_{\{3,4,5\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}), \end{aligned}$$

$$H(F_{3t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \leq H(F_{3t}|F_V^{t-1}),$$

$$\begin{aligned} &H(F_{5t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}, F_{\{3,4\}t}) + H(F_{\{3,4\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \\ &= H(F_{\{3,4,5\}t}|F_V^{t-1}, \tilde{Z}_{\{1,2\}}) \end{aligned}$$

Finally,

$$\begin{aligned} H(F_{\{1,2,4,5\}}) &= \sum_{t=1}^r H(F_{\{1,2,4,5\}t}|F_{\{1,2,4,5\}}^{t-1}) \\ &\geq \sum_{t=1}^r H(F_{\{1,2,4,5\}t}|F_V^{t-1}, F_{3t}) \\ &\geq \sum_{t=1}^r (a_t + b_t + c_t), \end{aligned}$$

which completes the proof.

2. Proofs of Theorems 7.1 and 7.2

PROOF (THEOREM 7.1) We prove the cases one by one:

- (i) We first show that an achieving scheme for the original scenario is an achieving scheme for the new scenario. To satisfy (3.5), the discussion by the original vocal untrusted user i can be done by the new vocal trusted helper i' . (3.7) and (3.8) still hold because there is no change to (A, D) . Hence, C_S does not decrease and R_S does not increase. To prove the reverse inequalities, consider an achieving scheme for the new scenario. By Proposition 3.1, it suffices to show that the scheme can be applied to the original scenario, with private randomization allowed for the untrusted user. To satisfy (3.5), the discussion and private randomization by the new user i' can be done by the original vocal untrusted user. (3.7) and (3.8) continue to hold trivially.
- (ii) Similar to the above case, the vocal user j can play the role of the removed trusted helper i in terms of private randomization and public discussion, and so (3.5) can be satisfied. (3.7) and (3.8) remain unchanged since (A, D) remains unchanged. ■

PROOF (THEOREM 7.2) It suffices to show that an achieving scheme for the original scenario can be applied to the new scenario.

- (i) (3.5) continues to hold as the set $V \setminus S$ of vocal users remains unchanged. (3.7) and (3.8) also hold as they can only be less stringent with (A, D) diminished.
- (ii) (3.5) continues to hold because the set $V \setminus S$ of vocal users becomes larger. (3.7) and (3.8) remain unchanged trivially. ■

REFERENCES

- [1] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec 2004.
- [2] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.
- [3] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sept 2013.
- [4] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless systems*, 2nd ed. Cambridge University Press, 2011.
- [5] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," in *2010 44th Annual Conference on Information Sciences and Systems (CISS)*, March 2010, pp. 1–6.
- [6] T. A. Courtade and T. R. Halford, "Coded cooperative data exchange for a secret key," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3785–3795, July 2016.
- [7] M. Mukherjee, N. Kashyap, and Y. Sankarasubramanian, "Achieving sk capacity in the source model: When must all terminals talk?" in *2014 IEEE International Symposium on Information Theory*, June 2014, pp. 1156–1160.
- [8] H. Zhang, Y. Liang, and L. Lai, "Secret key capacity: Talk or keep silent?" in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 291–295.
- [9] C. Chan, A. Al-Bashabsheh, J. Ebrahimi, T. Kaced, and T. Liu, "Multivariate mutual information inspired by secret-key agreement," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1883–1913, Oct 2015.
- [10] C. Chan, A. Al-Bashabsheh, J. B. Ebrahimi, T. Kaced, S. Kadhe, T. Liu, A. Sprintson, M. Yan, and Q. Zhou, "Successive omniscience," in *2015*

- International Symposium on Network Coding (NetCod)*, June 2015, pp. 21–25.
- [11] C. Chan, A. Al-Bashabsheh, Q. Zhou, N. Ding, T. Liu, and A. Sprintson, “Successive omniscience,” *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3270–3289, June 2016.
 - [12] C. Chan, “Generating secret in a network,” Ph.D. dissertation, Massachusetts Institute of Technology, 2010.
 - [13] M. Mukherjee and N. Kashyap, “The communication complexity of achieving SK capacity in a class of PIN models,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 296–300.
 - [14] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, “Secret key generation for a pairwise independent network model,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec 2010.
 - [15] S. Nitinawarat and P. Narayan, “Perfect omniscience, perfect secrecy, and steiner tree packing,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6490–6500, Dec. 2010.
 - [16] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam, “On the public communication needed to achieve SK capacity in the multiterminal source model,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3811–3830, July 2016.
 - [17] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “When is omniscience a rate-optimal strategy for achieving secret key capacity?” in *2016 IEEE Information Theory Workshop (ITW)*, Sept 2016, pp. 354–358.
 - [18] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography—Part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
 - [19] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
 - [20] M. Mukherjee, C. Chan, N. Kashyap, and Q. Zhou, “Bounds on the communication rate needed to achieve SK capacity in the hypergraphical source model,” in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 2504–2508.
 - [21] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar 2000.
 - [22] P. Gács and J. Körner, “Common information is far less than mutual information,” *Problems of Control and Information Theory*, vol. 2, no. 2, pp. 149–162, Feb. 1972.
 - [23] C. Chan, “The hidden flow of information,” in *2011 IEEE International Symposium on Information Theory Proceedings*, July 2011, pp. 978–982.
 - [24] N. Milosavljevic, S. Pawar, S. E. Rouayheb, M. Gastpar, and K. Ramchandran, “Deterministic algorithm for the cooperative data exchange problem,” in *2011 IEEE International Symposium on Information Theory Proceedings*, July 2011, pp. 410–414.
 - [25] C. Chan, “On tightness of mutual dependence upperbound for secret-key capacity of multiple terminals,” *arXiv preprint arXiv:0805.3200*, 2008.
 - [26] S. Fujishige, “Polymatroidal dependence structure of a set of random variables,” *Information and Control*, vol. 39, no. 1, pp. 55 – 72, 1978.
 - [27] R. W. Yeung, “A new outlook on Shannon’s information measures,” *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 466–474, May 1991.
 - [28] —, *Information Theory and Network Coding*. Springer, 2008.
 - [29] C. Chan and T. Liu, “Clustering by multivariate mutual information under chow-liu tree approximation,” in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2015, pp. 993–999.
 - [30] C. Chan, A. Al-Bashabsheh, Q. Zhou, T. Kaced, and T. Liu, “Info-clustering: A mathematical theory for data clustering,” *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 1, pp. 64–91, June 2016.
 - [31] C. Chan, A. Al-Bashabsheh, Q. Zhou, and T. Liu, “Duality between feature selection and data clustering,” in *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2016, pp. 142–147.
 - [32] A. Wyner, “The common information of two dependent random variables,” *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar 1975.
 - [33] W. Liu, G. Xu, and B. Chen, “The common information of N dependent random variables,” in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2010, pp. 836–843.
 - [34] T. S. Han, “Linear dependence structure of the entropy space,” *Information and Control*, vol. 29, pp. 337–368, 1975.
 - [35] Q. Chen, F. Cheng, T. Liu, and R. W. Yeung, “A marginal characterization of entropy functions for conditional mutually independent random variables (with application to wyner’s common information),” in *2015 IEEE International Symposium on Information Theory (ISIT)*, June 2015, pp. 974–978.
 - [36] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “Secret key agreement under discussion rate constraints,” *arXiv preprint arXiv:1701.05008*, 2017.
 - [37] C. Chan, A. Al-Bashabsheh, and Q. Zhou, “Incremental and decremental secret key agreement,” in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 2514–2518.
 - [38] I. Csiszár and P. Narayan, “Secrecy capacities for multiterminal channel models,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.
 - [39] M. Madiman and P. Tetali, “Information inequalities for joint distributions, with interpretations and applications,” *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2699–2713, June 2010.
 - [40] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, 2002.
 - [41] H. G. Eggleston, *Convexity*. CUP Archive, 1958, no. 47.